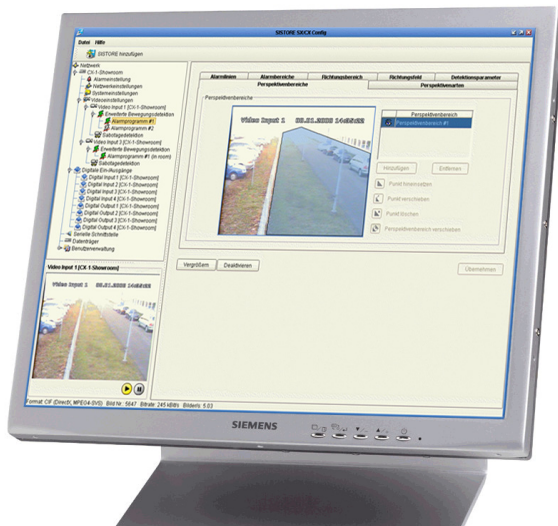# SIEMENS

SISTORE CX Config
SISTORE CX Swap-Out Config

Configuration Software

Configuration Manual

SISTORE CX V3.6

Building Technologies

Fire Safety & Security Products

About this document

This Configuration Manual contains instructions for the setup and configuration of SISTORE CX1, CX4, CX8 and FCV241 devices.

For information on operation please refer to the User Manual.

Orientation guide

| CX | SISTORE CX1, CX4 and CX8 functions |

| CX1 | SISTORE CX1 functions |

| CX4 | SISTORE CX4 functions |

| CX8 | SISTORE CX8 functions |

| FDV | Video Fire Controller FDV241 functions |

> **i** The Video Fire Controller FDV241 is also a product of the SISTORE product range.

Trademarks

SISTORE is a trademark of Siemens Fire & Security Products GmbH & Co. oHG.

Microsoft is a registered trademark and Windows a trademark of Microsoft Corporation.

All other product or company names mentioned in this document are trademarks or registered trademarks of their respective owners and are used only for purposes of identification or description.

Contacting us

If you have questions or suggestions regarding the product or this documentation, please contact our Customer Support centre:

Intranet: Customer Support Center

Internet: Worldwide contacts

Email: fs.support.sbt@siemens.com

Tel.: +49 89 9221 8000

Training courses

Siemens Building Technologies Fire Safety & Security Products provides training courses for all products.

Contents

1 Safety

1.1 Target readers

The instructions in this document are designed **only** for the following target readers:

Target readers	Qualification	Activity	Condition of the product
Operational startup personnel	Technical training for building or electrical installations as well as for network installations.	Puts the product into operation for the first time.	The product is not yet installed and configured.
Service personnel	Technical training for building or electrical installations as well as for network installations.	Checks the product at regular intervals to ensure that it is in good working order, services the product and repairs it.	Product already in use and requiring servicing.

1.2 Work safety information

- Read the general safety precautions before operating the device.
- Please also read the safety precautions for the devices that are operated by the software. Further information on this can be found in the Startup Manuals for the respective devices.
- Keep this document for reference.
- Always pass this document on together with the product.

1.2.1 Handling

Damage due to improper handling
- Protect the CD from scratching.
- To clean the CD use a soft dry cloth.

1.2.2 Transport

Damage during transport
- Always transport the CD in the case it originally came in.

1.2.3 Setup

Dangerous situation due to false alarm
- Make sure to notify all relevant parties and authorities providing assistance before testing the system.
- To avoid panic, always inform all those present before testing any alarm devices.

1.2.4 Installation

Data loss after software update
- Make sure to backup all data before updating the software.

1.2.5 Storage

Damage due to improper storage
- Always store the CD in its protective case.
- Keep the CD in an environment with a relative humidity of 10 – 90 %.
- Keep the CD between -5 and +55 °C.
- Do not store the CD in dusty places.
- Do not keep the CD close to sources of magnetic radiation.
- Protect the CD from moisture.
- Protect the CD from direct sunlight.

1.3 Meaning of the written warning notices

The severity of a hazard is indicated by the following written warning notices.

Signal word	Type of risk
CAUTION	There is a risk of minor to medium injuries or damage to property
IMPORTANT	Malfunctioning may result

1.4 Meaning of the hazard symbols

The nature of the hazard is indicated by icons.

Caution - Dangerous area!

Caution: Dangerous electrical voltage!

2 Technical data

2.1 SISTORE CX1

	CX1 0/25
General data	
Application	encoding and decoding of video signals, transmission, recording and evaluation
Power supply	12 – 24 V DC or 24 V AC, max. 1.25 A
Power consumption	max. 15 W
Ambient temperature (Tmra)	-10 to +50 °C
Relative humidity	20 – 80 % without condensation
Dimensions (W x H x D)	192 x 44 x 110 mm
Weight (without power supply unit)	0.95 kg
Battery	Varta 6032
Top-hat rail	mounting rail 35 x 7.5 mm to DIN EN 50022
Compact-flash card slot	CF-type I: 42.8 x 36.4 x 3.3 mm
Compact flash card	permissible temperature range: 0 – 70 °C
	min. transmission speed: 1 MB/s
	min. storage capacity: 4 GB
Connections and interfaces	
Operating modes, video input / video output (PAL)	1/0, 0/1
Audio input	1
Audio output	1
Digital inputs	2
Digital outputs	2
Ethernet	1 10/100 Mbit
Transparent serial data channel	1 RS485
Service port	1 USB 2.0
Internal hard drive(s)	–
Standards and protocols	
Transmission channel	10/100 Base-T
Video	MPEG4 SP/ASP, SVS
Audio	–
Network protocols	TCP, IP, HTTP, IGMP, ICMP, ARP, DHCP, SNMP, SSH, FTP, SCP, UpnP, CAP
Image formats	QCIF, CIF, 2CIF, DCIF, 4CIF
Video performance*	
QCIF CIF 2CIF DCIF 4CIF coding	25 ips
QCIF CIF 2CIF DCIF 4CIF decoding	25 ips
QCIF CIF 2CIF DCIF coding and decoding	25 ips
4CIF coding and decoding	25 ips
EDS tracking and encoding QCIF	25 ips

13

EDS tracking and encoding CIF	12.5 ips to 25 ips
EDS tracking and encoding 2CIF DCIF	6.25 ips to 12.5 ips
EDS tracking and encoding 4CIF	3.15 ips to 6.25 ips
ODR encoding QCIF	25 ips
ODR encoding CIF	25 ips
ODR encoding 2CIF DCIF	12.5 ips
ODR encoding 4CIF	6.25 ips
Number of video compression levels	5
Security functions	
Automatic connection on alarm	via IVM
Video signal disruption alarm	video loss detection
System operation possible without client PC	✓
Temperature monitoring	✓
Password protection	freely configurable
User permissions	freely configurable
Hardware watchdog	✓
Software watchdog	✓
Log file for all actions	✓
Administrative functions	
Integrated Web server	✓
Status display on the home page	✓
Firmware updatable via LAN	✓
Remote operation of internal functions	✓
Remote operation of peripheral devices	✓
IVM interface	✓
Recording and playback functions	
Pre-alarm ring buffer	✓
Alarm recording	✓
Rule manager	✓
Replay via software video decoder	✓
Remote replay via analogue monitor	✓
Search functions	✓
Streaming functions	
Transparent serial data channel	✓
Auto-connect video transmission	✓
Virtual cross bar	✓
Adjustable bandwidth	✓
Accessories	
Configuration software	✓
Software decoder	✓
Documentation: German, English, French and Spanish	✓
Top-hat rail mounting possible	✓

*   the ips data relate to the complete device

14

2.2 SISTORE CX4

	SISTORE CX4	SISTORE CX4 250	SISTORE CX4 500 / 1000
General data			
Application	transmission and reception	transmission, reception and recording	transmission, reception and recording
Operating voltage	12 V DC ± 5 %	12 V DC ± 5 %	12 V DC ± 5 %
Current consumption (continuous operation)	2.0 A	3.0 A	3.5 A
Current consumption (peak/startup current)		4.0 A	5.0 A
Ambient temperature (Tmra)	5 – 40 °C	5 – 40 °C	CX4 500: 5 – 40 °C CX4 1000: 5 – 35 °C
Relative humidity	20 – 80 % without condensation	20 – 80 % without condensation	20 – 80 % without condensation
Dimensions (W x H x D)	440 x 45 x 380 mm	440 x 45 x 380 mm	440 x 45 x 380 mm
Weight (without power supply unit)	4.2 kg	5.0 kg	5.8 kg
Connections and interfaces			
Video input/video output (PAL)	4/0 2/0 2/1 1/1 0/2	4/0 2/0 2/1 1/1 0/2	4/0 2/0 2/1 1/1 0/2
Audio input	(2)*	(2)*	(2)*
Audio output	(2)*	(2)*	(2)*
Digital trigger inputs	4	4	4
Digital relay outputs	4	4	4
10/100 Mbit Ethernet	1	1	1
RS232/RS485	1 (RS-232 or RS-485)	1 (RS-232 or RS-485)	1 (RS-232 or RS-485)
USB 1.1	1**	1**	1**
Compact Flash (internal)	1 (with operating system)	1 (with operating system)	1 (with operating system)
Internal hard drive	–	1 x 250 GB	CX4 500: 2 x 250 GB CX4 1000: 2 x 500 GB
Standards and protocols			
Transmission channel	10/100 Base-T	10/100 Base-T	10/100 Base-T
Video	MPEG4 technology	MPEG4 technology	MPEG4 technology
Audio	–	–	–
Network protocols	TCP, IP, HTTP, IGMP, ICMP, ARP, DHCP, SNMP, SSH, FTP, SCP, UpnP, CAP		
Image formats	QCIF, CIF, 2CIF, DCIF, 4CIF	QCIF, CIF, 2CIF, DCIF, 4CIF	QCIF, CIF, 2CIF, DCIF, 4CIF

Technical data

	SISTORE CX4	SISTORE CX4 250	SISTORE CX4 500 / 1000
Video performance*			
Encoding QCIF	100 ips	100 ips	100 ips
Encoding CIF	100 ips	100 ips	100 ips
Encoding 2CIF DCIF	100 ips	100 ips	100 ips
Encoding 4 CIF	50 ips	50 ips	50 ips
Decoding QCIF	50 ips	50 ips	50 ips
Decoding CIF	50 ips	50 ips	50 ips
Decoding 2CIF DCIF	50 ips	50 ips	50 ips
Decoding 4 CIF	50 ips	50 ips	50 ips
Encoding and decoding QCIF	50 ips and 25 ips	50 ips and 25 ips	50 ips and 25 ips
Encoding and decoding CIF	50 ips and 25 ips	50 ips and 25 ips	50 ips and 25 ips
Encoding and decoding 2CIF DCIF	50 ips and 25 ips	50 ips and 25 ips	50 ips and 25 ips
Encoding and decoding 4CIF	25 ips	25 ips	25 ips
EDS tracking and encoding QCIF	50 ips to 100 ips	50 ips to 100 ips	50 ips to 100 ips
EDS tracking and encoding CIF	25 ips to 50 ips	25 ips to 50 ips	25 ips to 50 ips
EDS tracking and encoding 2CIF DCIF	12.5 ips to 25 ips	12.5 ips to 25 ips	12.5 ips to 25 ips
EDS tracking and encoding 4CIF	4 ips to 12.5 ips	4 ips to 12.5 ips	4 ips to 12.5 ips
ODR encoding QCIF	100 ips	100 ips	100 ips
ODR encoding CIF	25 ips	25 ips	25 ips
ODR encoding 2CIF DCIF	12.5 ips	12.5 ips	12.5 ips
ODR encoding 4CIF	4 ips	4 ips	4 ips
Number of video compression levels	5	5	5
Security functions			
Automatic connection on alarm	via IVM	via IVM	via IVM
Video signal disruption alarm	✓	✓	✓
System operation possible without client PC	✓	✓	✓
Temperature monitoring	✓	✓	✓
Password protection	freely configurable	freely configurable	freely configurable
User permissions	freely configurable	freely configurable	freely configurable
Hardware watchdog	✓	✓	✓
Software watchdog	✓	✓	✓
Log file for all actions	✓	✓	✓

	SISTORE CX4	SISTORE CX4 250	SISTORE CX4 500 / 1000
Administrative functions			
Integrated Web server	✓	✓	✓
Status display on the home page	✓	✓	✓
Firmware updatable via LAN	✓	✓	✓
Remote operation of internal functions	✓	✓	✓
Remote operation of peripheral devices	✓	✓	✓
IVM interface	✓	✓	✓
Recording and playback functions			
Long time recording	–	250 GB HDD	CX4 500: 500 GB HDD CX4 1000: 1000 GB HDD
Pre-alarm ring buffer	–	✓	✓
Alarm recording	–	✓	✓
Rule manager	–	✓	✓
Replay via software video decoder	✓	✓	✓
Remote replay via analogue monitor	✓	✓	✓
Search functions	–	✓	✓
Streaming functions			
Transparent serial data channel	✓	✓	✓
Auto-connect video transmission	✓	✓	✓
Virtual cross bar	✓	✓	✓
Adjustable bandwidth	✓	✓	✓
Accessories			
Network cable, 3 m	✓	✓	✓
Power supply plug type	EU	EU	EU
Software for configuration	✓	✓	✓
Software decoder	✓	✓	✓
Documentation (DE/EN)	✓ / ✓	✓ / ✓	✓ / ✓
19" installation kit	✓	✓	✓
Desk-top housing kit	✓	✓	✓

*   not supported for SISTORE CX

**   for service purposes

***   the ips data relate to the complete device

2.3   SISTORE CX8

	SISTORE CX8	SISTORE CX8 500	SISTORE CX8 1000
General data			
Application	transmission and reception	transmission, reception and recording	transmission, reception and recording
Power source (integrated power supply)	100 – 230 V AC	100 – 230 V AC	100 – 230 V AC
Current consumption (continuous operation)	2.0 A	2.0 A	2.0 A
Current consumption (peak/startup current)	1.0 A	1.0 A	1.0 A
Ambient temperature (Tmra)	0 – 45 °C	5 – 45 °C	5 – 40 °C
Relative humidity	20 – 80 % without condensation	20 – 80 % without condensation	20 – 80 % without condensation
Dimensions (W x H x D)	430 x 87 x 370 mm	430 x 87 x 370 mm	430 x 87 x 370 mm
Weight (without power supply unit)	6.5 kg	8.0 kg	8.0 kg
Battery	Varta 6032	Varta 6032	Varta 6032
Connections and interfaces			
Video input/video output (PAL)	8/0 4/0 6/1 3/1 4/2 2/2 0/4	8/0 4/0 6/1 3/1 4/2 2/2 0/4	8/0 4/0 6/1 3/1 4/2 2/2 0/4
Audio input	(2)*	(2)*	(2)*
Audio output	(2)*	(2)*	(2)*
Digital trigger inputs	8	8	8
Digital relay outputs	8	8	8
10/100 Mbit Ethernet	1	1	1
RS485	1 (RS485)	1 (RS485)	1 (RS485)
USB 1.1	1**	1**	1**
Compact Flash (internal)	1 (with operating system)	1 (with operating system)	1 (with operating system)
Internal hard drive	–	2 x 250 GB	2 x 500 GB
Standards and protocols			
Transmission channel	10/100 Base-T	10/100 Base-T	10/100 Base-T
Video	MPEG4 technology	MPEG4 technology	MPEG4 technology
Audio	–	–	–
Network protocols	TCP, IP, HTTP, IGMP, ICMP, ARP, DHCP, SNMP, SSH, FTP, SCP, UpnP, CAP		
Image formats	QCIF, CIF, 2CIF, DCIF, 4CIF	QCIF, CIF, 2CIF, DCIF, 4CIF	QCIF, CIF, 2CIF, DCIF, 4CIF

	SISTORE CX8	SISTORE CX8 500	SISTORE CX8 1000
Video performance***			
Encoding QCIF	200 ips	200 ips	200 ips
Encoding CIF	200 ips	200 ips	200 ips
Encoding 2CIF DCIF	200 ips	200 ips	200 ips
Encoding 4 CIF	100 ips	100 ips	100 ips
Decoding QCIF	100 ips	100 ips	100 ips
Decoding CIF	100 ips	100 ips	100 ips
Decoding 2CIF DCIF	100 ips	100 ips	100 ips
Decoding 4 CIF	100 ips	100 ips	100 ips
Encoding and decoding QCIF	100 ips and 50 ips	100 ips and 50 ips	100 ips and 50 ips
Encoding and decoding CIF	100 ips and 50 ips	100 ips and 50 ips	100 ips and 50 ips
Encoding and decoding 2CIF DCIF	100 ips and 50 ips	100 ips and 50 ips	100 ips and 50 ips
Encoding and decoding 4CIF	50 ips	50 ips	50 ips
EDS tracking and encoding QCIF	100 ips to 200 ips	100 ips to 200 ips	100 ips to 200 ips
EDS tracking and encoding CIF	50 ips to 100 ips	50 ips to 100 ips	50 ips to 100 ips
EDS tracking and encoding 2CIF DCIF	25 ips to 50 ips	25 ips to 50 ips	25 ips to 50 ips
EDS tracking and encoding 4CIF	8 ips to 25 ips	8 ips to 25 ips	8 ips to 25 ips
ODR encoding QCIF	200 ips	200 ips	200 ips
ODR encoding CIF	50 ips	50 ips	50 ips
ODR encoding 2CIF DCIF	25 ips	25 ips	25 ips
ODR encoding 4CIF	8 ips	8 ips	8 ips
Number of video compression levels	5	5	5
Security functions			
Automatic connection on alarm	via IVM	via IVM	via IVM
Video signal disruption alarm	✓	✓	✓
System operation possible without PC	✓	✓	✓
Temperature monitoring	✓	✓	✓
Password protection	freely configurable	freely configurable	freely configurable
User permissions	freely configurable	freely configurable	freely configurable
Hardware watchdog	✓	✓	✓
Software watchdog	✓	✓	✓
Log file for all actions	✓	✓	✓
Administrative functions			
Integrated Web server	✓	✓	✓
Status display on the home page	✓	✓	✓
Firmware updatable via LAN	✓	✓	✓
Remote operation of internal functions	✓	✓	✓
Remote operation of peripheral devices	✓	✓	✓
IVM interface	✓	✓	✓

19

	SISTORE CX8	SISTORE CX8 500	SISTORE CX8 1000
Recording and playback functions			
Long time recording	–	2x 250 GB HDD	1000 GB HDD
Pre-alarm ring buffer	–	✓	✓
Alarm recording	–	✓	✓
Rule manager	–	✓	✓
Replay via software video decoder	✓	✓	✓
Remote replay via analogue monitor	✓	✓	✓
Search functions	–	✓	✓
Streaming functions			
Transparent serial data channel	✓	✓	✓
Auto-connect video transmission	✓	✓	✓
Virtual cross bar	✓	✓	✓
Adjustable bandwidth	✓	✓	✓
Accessories			
Network cable, 3 m	✓	✓	✓
Power supply plug type	EU	EU	EU
Software for configuration	✓	✓	✓
Software decoder	✓	✓	✓
Documentation (DE/EN)	✓ / ✓	✓ / ✓	✓ / ✓
19" installation kit	✓ optional	✓ optional	✓ optional
Desk-top housing kit	✓	✓	✓

*	not supported for SISTORE CX
**	for service purposes
***	the ips data relate to the complete device

2.4 Video Fire Controller FDV241

	FDV241 0/25
General data	
Application	encoding and decoding of video signals, transmission, recording and evaluation
Power supply	12 – 24 V DC or 24 V AC, max. 1.25 A
Power consumption	max. 15 W
Operating temperature	-10 to +50 °C
Relative humidity	20 – 80 % without condensation
Dimensions (W x H x D)	192 x 44 x 110 mm
Weight	0.95 kg
Battery	Varta 6032
Top-hat rail	mounting rail to DIN EN 50022
	35 x 7.5 mm; 2.3 mm thick
	– OR –
	35 x 15 mm; 2.3 mm thick
Compact-flash card slot	CF-type I: 42.8 x 36.4 x 3.3 mm
Compact flash card	permissible temperature range: 0 – 70 °C
	min. transmission speed: 1 MB/s r/w
	min. storage capacity: 4 GB
Connections and interfaces	
Operating modes, video input / video output (PAL)	1/0, 0/1
Audio input	1
Audio output	1
Digital inputs	2
Digital outputs	2
Ethernet	1 10/100 Mbit
Transparent serial data channel	1 RS485
Service port	1 USB 2.0
Internal hard drive(s)	–
Standards and protocols	
Transmission channel	10/100 Base-T
Video	MPEG4 SP/ASP, SVS
Audio	–
Network protocols	TCP, IP, HTTP, IGMP, ICMP, ARP, DHCP, SNMP, SSH, FTP, SCP, UpnP, CAP
Image formats	QCIF, CIF, 2CIF, DCIF, 4CIF
Video performance*	
QCIF CIF 2CIF DCIF 4CIF coding	25 ips
QCIF CIF 2CIF DCIF 4CIF decoding	25 ips
QCIF CIF 2CIF DCIF coding and decoding	25 ips

Technical data

	FDV241 0/25
4CIF coding and decoding	25 ips
Number of video compression levels	5
Security functions	
Automatic connection on alarm	via IVM
Video signal disruption alarm	video loss detection
System operation possible without client PC	✓
Temperature monitoring	✓
Password protection	freely configurable
User permissions	freely configurable
Hardware watchdog	✓
Software watchdog	✓
Log file for all actions	✓
Administrative functions	
Integrated Web server	✓
Status display on the home page	✓
Firmware updatable via LAN	✓
Remote operation of internal functions	✓
Remote operation of peripheral devices	✓
IVM interface	✓
Recording and playback functions	
Pre-alarm ring buffer	✓
Alarm recording	✓
Rule manager	✓
Replay via software video decoder	✓
Remote replay via analogue monitor	✓
Search functions	✓
Streaming functions	
Transparent serial data channel	✓
Auto-connect video transmission	✓
Virtual cross bar	✓
Adjustable bandwidth	✓
Accessories	
Configuration software	✓
Software decoder	✓
Documentation: German, English, French and Spanish	✓
Top-hat rail mounting possible	✓
Standards	
Protection rating	EN 60529
	IP20
EMC	EN 61000-6-4
	EN 50130-4

	FDV241 0/25
QA standards	Siemens Standard SN 36350
	ISO9001
	ISO9004
CE Conformity Marking	yes
Connection to detector bus FDCC221	
Connections	design: plug-type connection
	cross-section: 0.2 – 1.5 mm^2
Operating voltage	12 – 33 V DC
Operating current (closed circuit)	0.6 – 0.75 mA
Operating temperature	-10 to +55 °C
Relative humidity	≥ 95 % rel. (at T = 25 ±3 °C)
	93 % rel. (at T = 40 ±2 °C)
	temporary condensation permissible
Maximum current connection factor	3
Quiescent current connection factor	3
Address connection factor	1
Separator connection factor	1
Protocol	FDnet
Compatibility	for details see Doc. No. 008331 'List of compatibility'
External alarm indicator	
Connector for external alarm indicator	none
Standards	
CPD	EN 54-17
	EN 54-18

* the ips data relate to the complete device

23

3 Setup

3.1 Operating modes and performance characteristics

The operating mode determines how many video inputs and outputs are available. Unavailable video inputs and outputs are not shown in the SISTORE CX Config and SISTORE CX Client applications.

The operating modes for the SISTORE devices are set using the configuration software (SISTORE CX Config).

ℹ️ Remote video sources are available only at SISTORE devices with a storage medium. See Section: 11 Configuring the storage medium.

| CX1 | FDV |

Operating mode	Video input	Video output	4CIF	2CIF / DCIF	CIF	QCIF	Remote video sources*
Enhanced-performance encoder	1	0	max. 25 ips	max. 25 ips	max. 25 ips	max. 25 ips	–
Standard-performance decoder	0	1	max. 25 ips	max. 25 ips	max. 25 ips	max. 25 ips	–
EDS enhanced-performance tracking and encoder	1	0	max. 3.12 ips	max. 6.25 ips	max. 12.5 ips	max. 25 ips	–
EDS standard-performance tracking and encoder	1	0	max. 6.25 ips	max. 12.5 ips	max. 25 ips	max. 25 ips	–
ODR and standard-performance encoder	1	0	max. 6.25 ips	max. 12.5 ips	max. 25 ips	max. 25 ips	–

| CX4 |

Operating mode	Video input	Video output	4CIF	2CIF / DCIF	CIF	QCIF	Remote video sources*
Standard-performance encoder	4	0	max. 12.5 ips	max. 25 ips	max. 25 ips	max. 25 ips	1
Enhanced-performance encoder	2	0	max. 25 ips	max. 25 ips	max. 25 ips	max. 25 ips	1
Enhanced-performance encoder/decoder	1	1	max. 25 ips	max. 25 ips	max. 25 ips	max. 25 ips	2
Standard-performance encoder/decoder	2	1	max. 12.5 ips (output also max. 25 ips)	max. 25 ips	max. 25 ips	max. 25 ips	2
Standard-performance decoder	0	2	max. 25 ips	max. 25 ips	max. 25 ips	max. 25 ips	–
EDS enhanced-performance tracking and encoder	2	0	max. 3.12 ips	max. 6.25 ips	max. 12.5 ips	max. 25 ips	2
EDS standard-performance tracking and encoder	2	0	max. 6.25 ips	max. 12.5 ips	max. 25 ips	max. 25 ips	2
EDS standard-performance tracking and encoder	4	0	max. 1 ips	max. 3.12 ips	max. 6.25 ips	max. 25 ips	2
ODR and standard-performance encoder	4	0	max. 1 ips	max. 3.12 ips	max. 6.25 ips	max. 25 ips	2

* the number refers to 4CIF/25 ips

CX8

Operating mode	Video input	Video output	4CIF	2CIF / DCIF	CIF	QCIF	Remote video sources*
Enhanced-performance encoder	4	0	max. 25 ips	max. 25 ips	max. 25 ips	max. 25 ips	2
Enhanced-performance encoder/decoder	2	2	max. 25 ips	max. 25 ips	max. 25 ips	max. 25 ips	4
Enhanced-performance encoder/decoder	3	1	max. 25 ips	max. 25 ips	max. 25 ips	max. 25 ips	3
Standard-performance encoder	8	0	max. 12.5 ips	max. 25 ips	max. 25 ips	max. 25 ips	2
Standard-performance encoder/decoder	6	1	max. 12.5 ips (output also max. 25 ips)	max. 25 ips	max. 25 ips	max. 25 ips	3
Standard-performance encoder/decoder	4	2	max. 12.5 ips (output also max. 25 ips)	max. 25 ips	max. 25 ips	max. 25 ips	4
Standard-performance decoder	0	4	max. 25 ips	max. 25 ips	max. 25 ips	max. 25 ips	–
EDS enhanced-performance tracking and encoder	4	0	max. 3.12 ips	max. 6.25 ips	max. 12.5 ips	max. 25 ips	4
EDS standard-performance tracking and encoder	4	0	max. 6.25 ips	max. 12.5 ips	max. 25 ips	max. 25 ips	4
EDS standard-performance tracking and encoder	8	0	max. 1 ips	max. 3.12 ips	max. 6.25 ips	max. 25 ips	4
ODR and standard-performance encoder	8	0	max. 1 ips	max. 3.12 ips	max. 6.25 ips	max. 25 ips	4

* the number refers to 4CIF/25 ips

3.2 SISTORE in a system network

CX FDV

SISTORE devices can also be operated in a network of systems.

This network of systems can have the following software as its central component: SISTORE CX Client or IVM Client.

Number of SISTORE CX devices in a network of systems	max. 100
Number of SISTORE CX Clients in a network of systems	no limit
Number of SISTORE CX Clients logged on simultaneously to the same SISTORE CX device	max. 5
Number of IVM WEB Clients in a network of systems	no limit
Number of IVM WEB Clients logged on simultaneously to the same SISTORE CX device	max. 5
Number of live image playbacks at highest quality per device	max. 12

- Each recording being played will reduce the number of live images by one.
- The number of live images is reduced in proportion to the bandwidth.

3.3   Software included with the system

| CX | FDV |

The accompanying CD contains documentation as well as the software needed to run the SISTORE device:

- SISTORE CX client
- Adobe Acrobat Reader
- DirectX 9
- Java 2 Runtime Environment
- SISTORE Player
- SISTORE CX Config
- SISTORE Swap-Out Config

Software for configuration

The following software is currently available for configuring the various components:

SISTORE CX Client	• Rule configuration
SISTORE CX Config	• Creating the SISTORE device list
	• Configuring motion detection
	• Configuring Enhanced Motion Detection
	• Configuring the detection of removed or left objects
	• Configuring tamper detection
	• User administration / configuration
SISTORE Swap-Out Config	• Video swap-out

3.4   Setting the IP address of the client PC

| CX | FDV |

1.   Select **Start** > **Settings** > **Control Panel** > **Network Connections** in the Windows start menu.
2.   Right-click on the selected network connection.
3.   Select **Properties** in the context menu.
   → The **Local Area Connection Properties** dialog box appears.
4.   Select the Internet protocol **TCP/IP**.
5.   Click on **Properties**.
   → The **Internet Protocol (TCP/IP) Properties** dialog box appears.
6.   Activate the option **Use the following IP address**.
7.   Enter 169.254.xxx.xxx for the **IP address** and **255.255.0.0 for the subnet mask**.
8.   Click **OK**.
9.   Restart your client PC.
   → The device is now ready for software installation. See Section 3.14 Installing the software.

3.5 Set date and time of client PC

CX FDV

1. Select **Start > Settings > Control Panel > Date/Time** in the Windows start menu.
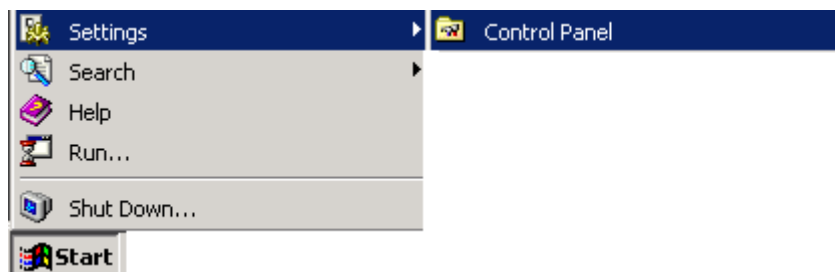
Fig. 1   Setting date and time of the Client PC via the Windows start menu

2. Adjust the time of your client PC to the time zone where your PC is run, e.g. GMT + 01:00 Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna. See Section: 7.3 Synchronizing the time on SISTORE devices.

3.6 Define an NTP Server within a network

CX FDV

The time on your client PCs within a network can be synchronized with the time on the NTP Server. See Section: 3.7 Synchronizing the time on the client PC with the time on the NTP server and Section: 7.3 Synchronizing the time on SISTORE devices.

Within a network, you can declare a client PC to be the NTP Server. If the PC is a member of a domain, the domain controller of the network should be declared the NTP Server. If the PC is a member of a workgroup, please install your own NTP Server.

The accompanying SISTORE CX Client CD contains a software for setting up your own NTP Server.

ⓘ   The client PC you want to declare an NTP Server within a network should always be switched on.

3.7   Synchronizing the time on the client PC with the time on the NTP server

CX FDV

An NTP Server always provides the current time. The time of your client PC will be updated continuously with the time from the NTP Server.

This is a periodic synchronization mode, i.e. the time is updated at regular intervals. This may take several hours.

Prerequisite:

In order to synchronize the time on your client PC with the time on an NTP server, the IP address of the NTP Server must be specified.

1.   Select **Start > Programs > Accessories > Command Prompt** in the Windows start menu.
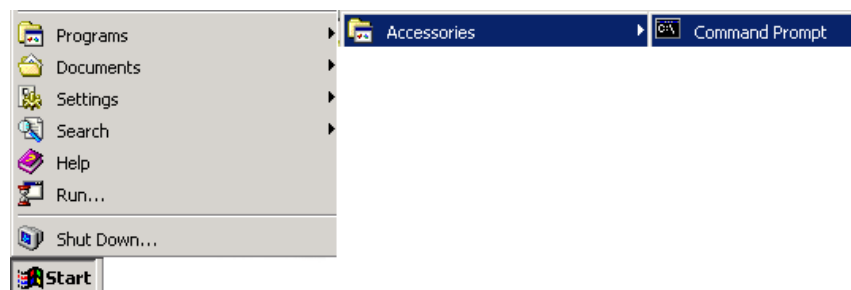
Fig. 2   Open command prompt from the Start menu

2.   Enter the following command in the command prompt window:

       net time /setsntp:xxx.xx.xx.xxx

       Enter the IP address of the NTP Server for xxx.xx.xx.xxx.

3.   Restart your client PC or enter the following command in the command prompt of your PC:

       net stop w32time
       net start w32time

4.   Select **Start > Settings > Control Panel > Administrative Tools > Services > Windows Time** in the Windows start menu.

→ The **Windows Time Properties** dialog box appears:
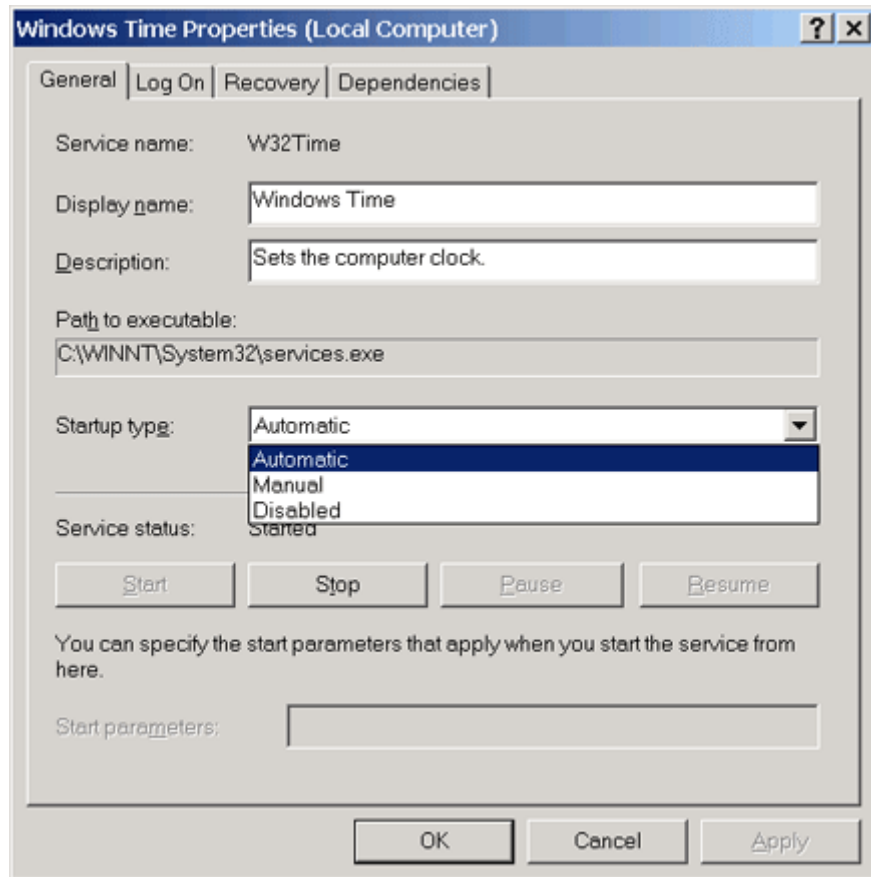
Fig. 3   "Windows Time Properties" dialog

5.   Select the **General** tab.

6.   Select **Automatic** in the Startup type list box.

→ When your client PC is started, a connection to the NTP server will be established automatically. See Section: 7.3 Synchronizing the time on SISTORE devices.

3.8   Network settings of client PC

| CX | FDV |

Configure the network settings of your client PC to use a DHCP server (even if there is none on the network). Your client PC and the SISTORE devices will then automatically find an IP address in the address range 169.254.x.x with the subnet mask 255.255.0.0.
This automatically assigned IP address must then be adapted to your needs with the SISTORE CX Config application.

→ Please check if your client PC and the SISTORE have found an IP address in the specified address range. If this is not the case please assign manually an IP address to your SISTORE devices.

3.9 Connecting digital inputs and outputs

1. See Section: 14.6.2 Definition of the alarm handling and Section: 6 Alarm settings configuration.
2. Connect the devices to the digital inputs and outputs in the following manner:

Digital inputs

CX1 FDV
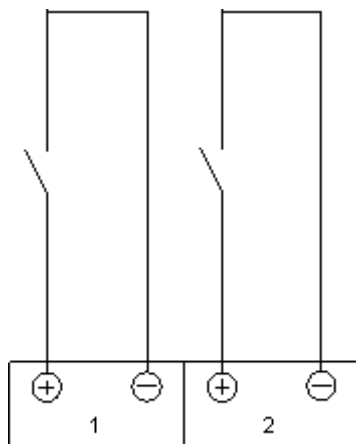
CX4 CX8
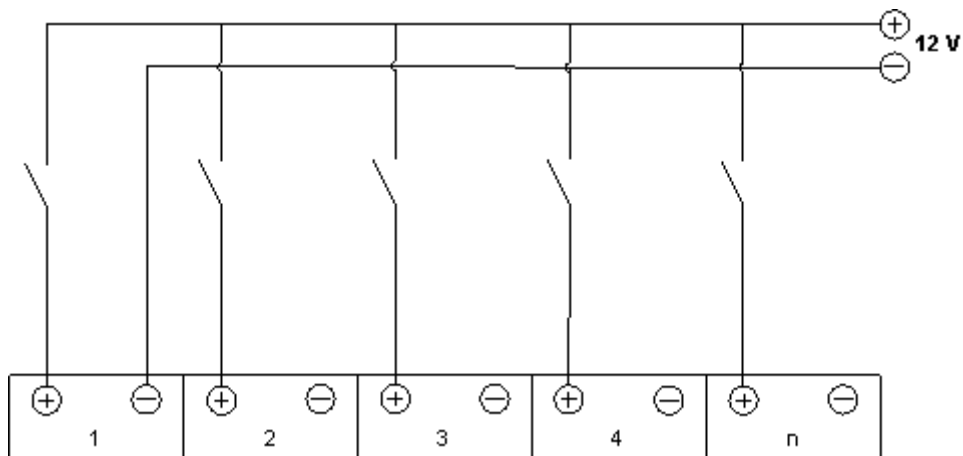
CX

Digital outputs
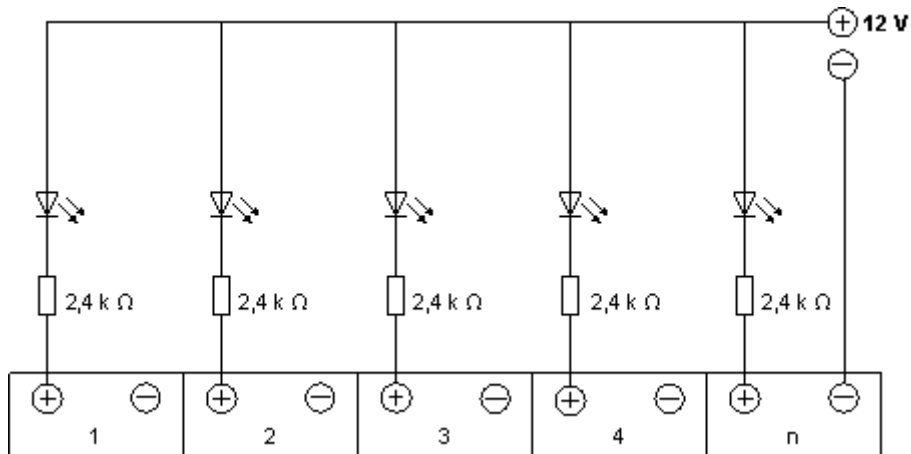
3.10　Connecting a RAID system

CX8

1. Connect a RAID system to the SCSI port.
2. SISTORE RAID V1.0 has been tested by Siemens. Please refer to the Configuration Manual for SISTORE RAID V1.0.
3. Configure the RAID system. See Section: 11 Configuring the storage medium.

3.11　Protocols and devices that have been tested

CX　FDV

Protocol/device	Pan/tilt function	Camera positions	Focus and zoom	OSD menu	Variable speed	Bidirectional bus wiring
CCDA protocol	✓	✓	✓		✓	
CCDA1410	✓	✓	✓		✓	
CCDA1415	✓	✓	✓	✓	✓	
CCDA1425	✓	✓	✓	✓	✓	
CCDA1435	✓	✓	✓	✓	✓	
SCU protocol (V2.2)	✓	✓	✓		✓	
Pan-and-tilt drive CDD2410	✓	✓			✓	
Pan/tilt head PT40 with controller CDC0501	✓					
Pan/tilt head PT40 with controller CDC0502	✓	✓				
PANASONIC protocol	✓	✓	✓	✓	✓	✓
SIVIS Mini Dome	✓	✓	✓	✓	✓	✓
Panasonic WV-CS950	✓	✓	✓	✓	✓	✓
PELCO-D protocol	✓	✓	✓		✓	✓
Pelco Spectra III	✓	✓	✓		✓	
CCDA1435 - Pelco	✓	✓	✓		✓	
Pelco Spectra IV (firmware version lower than 1.062)	✓	✓	✓		✓	
Pelco Spectra IV (firmware version 1.062 or higher)	✓	✓	✓		✓	
Molynx protocol V3 (SISTORE CX V3.1 or higher)	✓	✓	✓	✓	✓	
CCDS1415	✓	✓	✓	✓	✓	
RX217 & CCAC1415-LPI	✓	✓	(✓) Only with Siemens cameras: CCAC1415-LPI	(✓)	✓	
LEDERER protocol (SISTORE CX V3.1 or higher)	✓	✓	(✓) Only with Siemens cameras: CCBC1225-LP and CCBS1225-LP	(✓)	✓	✓
Lederer & CCBC1225-LP / CCBS1225-LP	✓	✓	(✓) Only with Siemens cameras: CCBC1225-LP and CCBS1225-LP	(✓)	✓	✓

3.12 Examples of system configurations

3.12.1 Default settings in SISTORE CX Config

CX FDV

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. Please note the configurations in the following sections. See Section: 10.1 Serial port operation modes, Section: 10.2 Serial port settings and Section: 8.4.4 Activating/deactivating camera control functions.

3.12.2 Dome CCDA1410 / CCDA1415 / CCDA1425 / CCDA1435

CX FDV
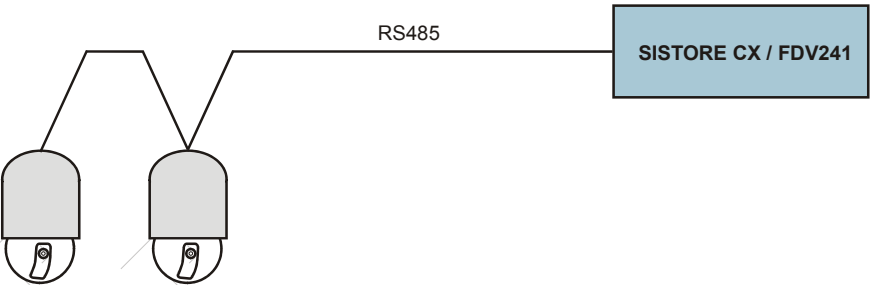
Connections

Signal	SISTORE CX 9-pin Sub-D socket	CCDA1410 / CCDA1415 / CCDA1425 / 1435
A (Rx/Tx +)	2	Data +
B (Rx/Tx -)	3	Data -

1. Connect the Dome to the RS485 port (COM2) of the SISTORE device.
2. Please also refer to the product documentation for the Dome.

i Make sure that the dome camera is configured for **RS485 two-wire operation**.

3.12.3   SCU pan/tilt head PT40P

CX FDV
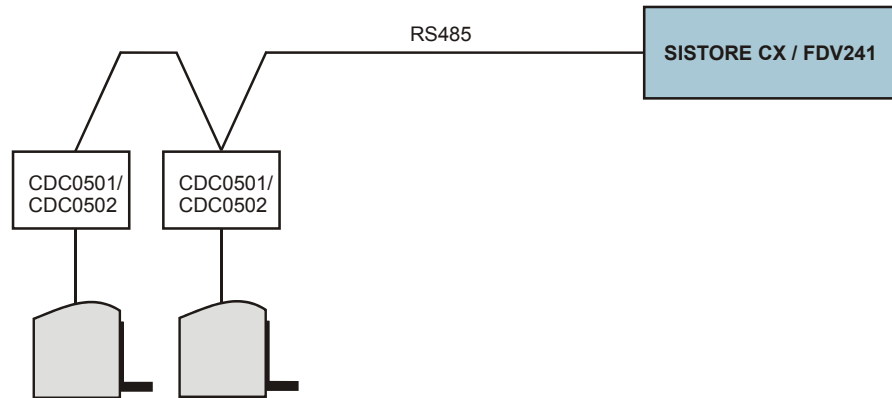
1.   Connect the pan/tilt heads via the controller CD0502 to the RS485 port (COM2) of the SISTORE device.

2.   Please also refer to the product documentation for the pan/tilt head.

Connections

Signal	SISTORE CX 9-pin Sub-D socket	CDC0502	CDC0501	PT40P
A (Rx/Tx +)	2	Rx/Tx +	Rx/Tx -	Data +
B (Rx/Tx -)	3	Rx/Tx -	Rx/Tx -	Data -

3.12.4   Pan-and-tilt drive CDD2410

CX FDV
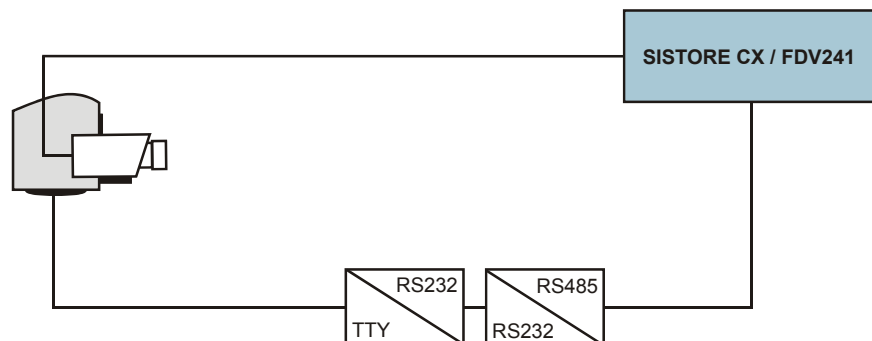
1.   Connect the pan-and-tilt drive to the SISTORE device (COM2).

2.   Connect the camera to the SISTORE device (video input).

3.   Please also refer to the instruction manuals for the pan-and-tilt head, the converter and the camera.

Connections

Signal	SISTORE CX 9-pin Sub-D socket	TTY/RS232 converter	RS232 to RS485 interface converter	CDD2410
A (Rx/Tx +)	2	1	1	Data +
B (Rx/Tx -)	3	2	2	Data -

3.13 System requirements for the client PC

| CX | FDV |

The PC on which the SISTORE CX Client software is installed should meet the following requirements:

Processor	Dual-core processor
RAM	1 GB
Available hard drive capacity	5 GB
Operating system	Windows XP SP2 or Windows Vista
Graphics card	With support for DirectX 8 (or later version)
Screen resolution	Min. 1024 x 768 pixels
Colour depth	16 bit or 32 bit (24 bit not supported)

NOTE

Improvements in the performance of live video display and recording can be achieved by expanding the hardware used (high-performance processors, graphics cards, internal memories).

3.14 Installing the software

| CX | FDV |

1. Place the CD in the CD drive of the client PC.
   → The installation program is started automatically.
2. Follow the instructions of the installation program.

Software cannot be executed

IMPORTANT   The client PC has to be restarted following installation or uninstallation of the software as otherwise the application will not run.

Restart the client PC when you are prompted to do so.

→ The following software applications are now installed:
   – SISTORE CX Config
   – SISTORE CX Swap-Out Config
   – SISTORE CX Client
   – SISTORE CX Player

3.15   Starting the software

CX FDV

1. Select **Start** > **Programs** > **SIEMENS Video Software Suite** in the Windows start menu.
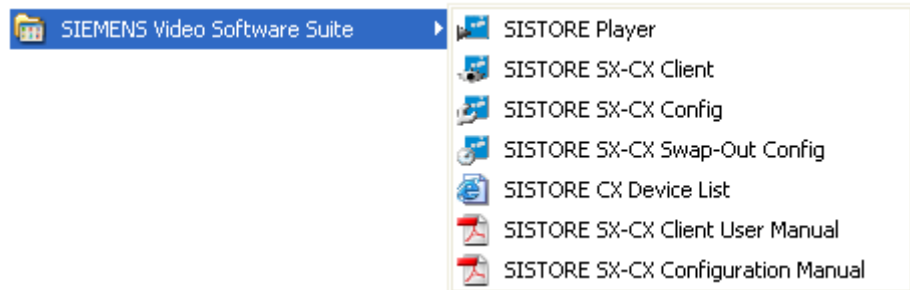
Fig. 4   SISTORE Start menu

– OR –

Click on the appropriate desktop shortcut.
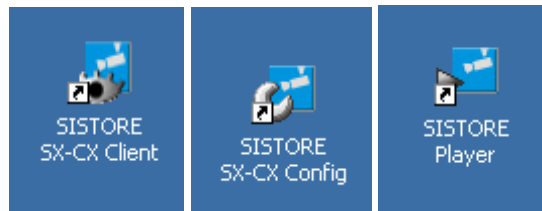
Fig. 5   SISTORE desktop shortcut

2. Log on to the server using the following user name and password.

	SISTORE CX Client	**SISTORE CX Config**	**SISTORE CX Swap-Out Config**
User name	admin	admin	admin
Password	admin	admin	admin
Host name	Prerequisite: A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device. **[all]** or an individual SISTORE device		Prerequisite: A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device. The user is assigned the following rights. The Admin has these rights by default. ● Recording: Search for recordings ● Recording: Lock recording ● Storage: Show configuration ● Streaming method: Use video input ● User administration: Show

i   We recommend changing the passwords in the SISTORE CX Client after the first login.

3.15.1   Starting the SISTORE CX Swap-Out Config software

Windows XP

1.   Log on as an administrator.
2.   Start the SISTORE CX Swap-Out Config application.

Windows Vista

1.   Log on as an administrator.
2.   Select **Start** > **Programs** > **SIEMENS Video Software Suite** in the Windows start menu.
3.   Right-click on **SISTORE CX Swap-Out Config**.
4.   Select **Properties**.
5.   Select the **Compatibility** tab.
6.   Mark the checkbox **Run program as administrator**.
7.   Click **OK**.

3.16 Selecting manuals

CX FDV

The following manuals are available:

- SISTORE CX Client User Manual
- SISTORE CX Configuration Manual

1. Select **Start** > **Programs** > **SIEMENS Video Software Suite** in the Windows start menu.
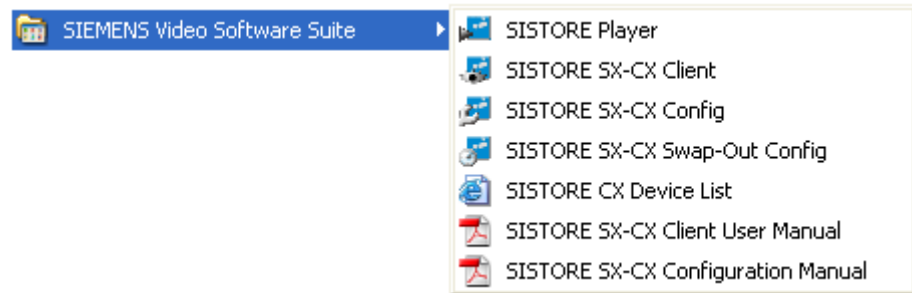
Fig. 6   SISTORE Start menu

2. Select a manual.

3.17 Symbols in SISTORE CX Config

CX FDV

The SISTORE devices added to the device list using SISTORE CX Config will be displayed in the tree view as follows:

Symbol	Meaning
	The device is offline (no network connection)
	The device is online, a user with configuration permission is logged on.
	The device is online, a user without configuration permission is logged on.
	The device is online, no user is logged on. (Login information incorrect)
	The device is online, a user is logged on, the firmware or software version is obsolete.
	The video service utilities are restarted. E.g. for recordings and live video.
	The device is restarted. E.g. after a firmware update or activation of an internal RAID.
	The configuration settings of the SISTORE CX Client are not consistent with the settings of SISTORE CX Config.
	The update is carried out by another user.
	The device is not ready for use; the firmware needs to be updated. See Section: 4.4 Firmware update.
	The device is not ready for use; wrong update version, the firmware needs to be updated once more. See Section: 4.4 Firmware update.

4 Initial configuration

4.1 Connecting to SISTORE device

CX FDV

1. Start the **SISTORE CX Config** application.
   ➔ The **SISTORE CX Config** dialog box opens.
2. Click the icon **Add SISTORE** in the toolbar.
   ➔ The "SISTORE Selection Wizard" will appear.
3. Click **Next >**.

Fig. 7   SISTORE Selection Wizard

4. Select a device from the list box on the left.
   – OR –
   Enter the IP address of the device into the input field on the left.
5. Click **Add**.
6. Click **Next >**.
7. Log in using the following information:
   User name: admin **Password**: admin.
8. Click on **Finish**.
   ➔ The connection to the SISTORE device has been established.
   ➔ The device list **serverlist.xml** will be created.
9. Open the **SISTORE CX Client** application software.

4.2 Disconnecting a SISTORE device

CX FDV

1. Right-click on a SISTORE device in the tree view.
2. Select **Remove** in the context menu.
    ➔ The SISTORE device has been disconnected.
    ➔ The device list **serverlist.xml** will be updated automatically.
    ➔ The SISTORE device is no longer assigned to a device group.

4.3 Using the device list (serverlist.xml)

CX FDV

1. Copy the device list **serverlist.xml** in the directory **D:\Cevis\SISTORE_SX_Client** of your client PC.
2. Paste the device list into the directory **D:\Cevis\SISTORE_SX_Client** of other client PCs.

4.4 Firmware update

CX FDV

Prerequisites:

There is a minimum network bandwidth of 10 Mbit/s between the client PC and the SISTORE CX device.

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

Symbols in the tree view

The update is carried out by another user.

The firmware needs to be updated. The device is not ready for use.

Wrong update version; the firmware needs to be updated once more. The device is not ready for use.

Updating the device

i	**NOTE** ● Do not update more than five devices at a time. ● It is recommended to back up the SISTORE configuration before starting a firmware update. See Section 5.1 Saving SISTORE configurations.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.

2. Select the menu sequence **File > Firmware Update**.

➔ The dialog box **Firmware Update** lists all the devices that can be accessed on the network.

Select	Host name	Type	Serial no.	Version	Actions	Device State	Progress
false	cx-05031234	CX4	05031234	3.5.0.04.20...		Device ready	0
false	CX-1-Showroom	CX4	04020019	3.4.0.15.20...		Device ready	0
false	CX-2-Showroom	CX4	04080012	3.4.0.15.20...		Device ready	0
false	CX_Showroom...	CX4	04060002	3.4.0.15.20...		Device ready	0
false	hus-04090016	CX4	04090016	3.5.0.04.20...		Device ready	0
false	swtest-cx1-58	CX1	07010007	3.5.0.05.20...		Device ready	0
false	swtest-cx4-53	CX4	04090018	3.5.0.06.20...		Device ready	0

CX1 [   ] 📂

CX4/CX8 [   ] 📂

Start Firmware Update

Factory Reset   Restart Device   Shutdown Device

Fig. 8   "Firmware Update" dialog box

3. Select the device you want to update in the **Select** column.

4. Click the folder symbol corresponding to the device type (CX1 or CX4/CX8).

i	**NOTE** The Video Fire Controller FDV241 uses the SISTORE CX1 firmware.

5. Select the current update file from the **Open** dialog box.

6. Confirm by clicking **Open**.

7. Click the **Start Firmware Update** button.

➔ The **Progress** column will show the processing status of the update procedure.

➔ The dialog box can be closed only after the firmware update is completed.

4.5 Reset to factory default settings

CX FDV

⚠	**IMPORTANT**	**Data loss after resetting to factory default settings**
		After a reset, all factory defaults will be restored.
		● Make sure that all relevant configuration data has been backed up (see Section: 5.1 Saving SISTORE configurations).

1. Select a device in the **Select** column (see Fig. 8).
2. Click the **Factory Reset** button.

4.6 Shutting down / restarting a device

CX FDV

⚠	**IMPORTANT**	**Loss of recorded video data**
		When shutting down or restarting the device, current recordings will be stopped.
		● Make sure not to interrupt a current recording process.

⚠	**IMPORTANT**	**Restart of the device**
		When the device has been shut down, it can only be restarted manually.
		● Make sure that the device can be restarted manually.

1. Select a device in the **Select** column (see Fig. 8).
2. Click the **Shutdown Device** or the **Restart Device** button.
3. Restart the device (manually).

4.7   SISTORE domain server activation

| CX | FDV |

The SISTORE domain server enables global user administration.

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2.   Click **Network** in the tree view.
3.   Select the **Domain Settings** tab.
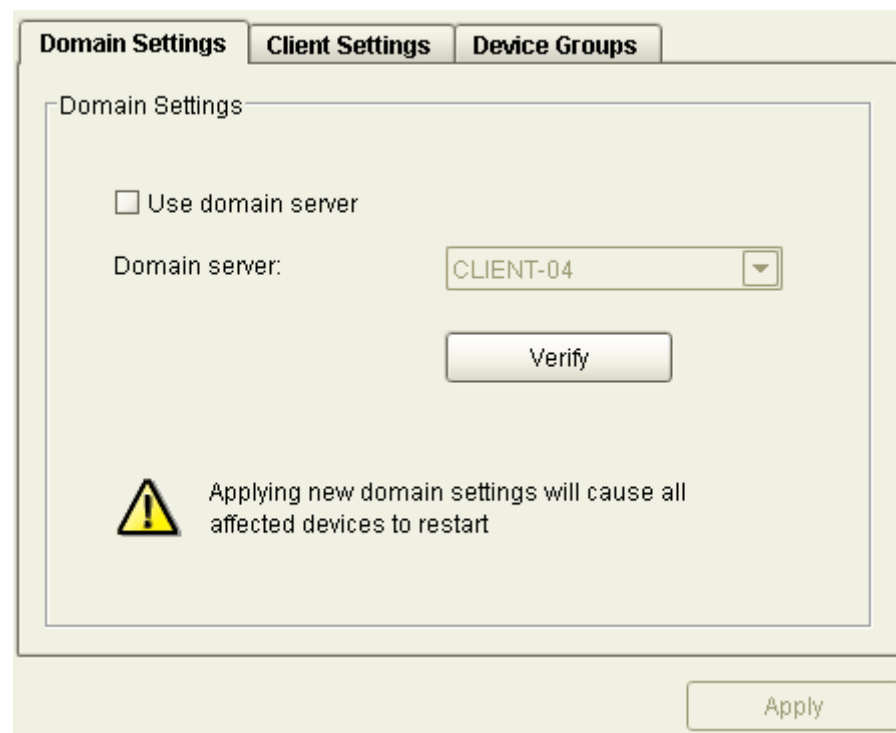
Fig. 9   Network – Domain Settings

4.   Tick the checkbox **Use domain server**.
5.   Click on **Verify** if you require information on which of the SISTORE devices a domain server has been defined for.
6.   Select the server PC in the **Domain server** list box.
7.   Click **Apply**.
8.   Answer **Yes** in the confirmation dialog.
    ➔ The SISTORE devices will be restarted.

4.8 Client settings

CX FDV

Prerequisite:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. Click **Network** in the tree view.
3. Select the **Client Settings** tab.
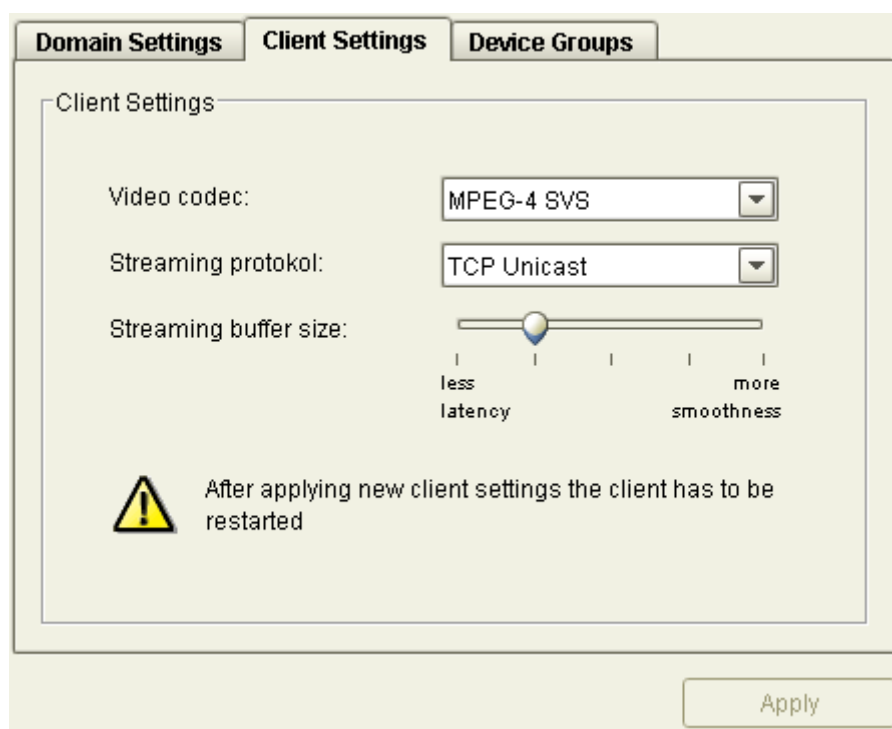
Fig. 10   Network – Client Settings

4. Make the following settings (see Section: 5.1 Saving SISTORE configurations).

Streaming method	Selection possibilities
Codec	MPEG-4 SVS – SIEMENS Video Streams
	MPEG-4 SPASP – "International Standard ISO/IEC 14496 2 Part 2: Visual"
Streaming protocol	TCP Unicast
	RTP Multicast
Streaming buffer size	Less latency: Delays in the video stream
	More smoothness: Consistent, smooth video stream

5. Click **Apply**.

4.9 Defining and deleting device groups

CX FDV

SISTORE device can be assigned to groups. These device groups will be loaded when the SISTORE CX Client is started and can be connected individually.

> **i**   In an environment with a large number of SISTORE devices we recommend defining device groups and connecting only the group of devices actually required. Further information on this can be found in the SISTORE CX Client User Manual.

Defining device groups

> **i**   Each device can only be assigned to one group.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
3. Click **Network** in the tree view.
4. Select the **Device Groups** tab.
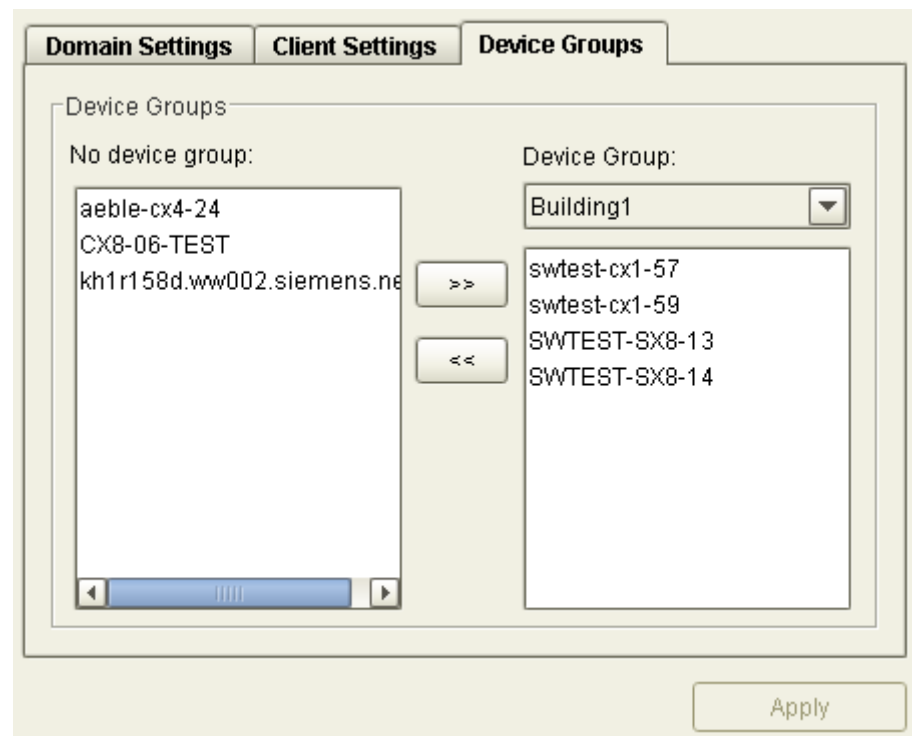
Fig. 11   Network – Device groups

5. Select <New group> in the **Device Group** drop-down list.
   ➔ A cursor flashes in the **Device Group** drop-down list.
6. Enter the name of the new device group here.
7. To assign devices to a device group, select one or several devices in the **No device group** list box.
8. Click on **>>**.

➔ The devices appear in the **Device Group** list box and have been assigned to the device group.

9. Click **Apply**.

Deleting a device group

You can delete a device group by removing all the devices assigned to that group from the list.

1. Select the group you want to delete in the **Device Group** drop-down list.

2. Select all the devices assigned to this device group.

3. Click on **<<**.

➔ The devices appear in the **No device group** list box and are no longer assigned to the device group.

4. Click **Apply**.

5 Saving and loading configurations

5.1 Saving SISTORE configurations

[CX] [FDV]

Prerequisite:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

---

i

- PTZ camera positions are not saved.
- If the SISTORE device is not provided with an internal or external hard drive, the camera and scheduler configurations will not be saved.
- Network settings and storage media selections are not saved. See Sections 7.1 Configuring network settings and 11 Configuring the storage medium.

---

1. In the tree view, navigate to a SISTORE device.
2. Click **Save configuration**.

Fig. 12   SISTORE configuration data – Save configuration

➔ The **Import/Export status** window opens.

3. To ensure that all the configuration information is exported correctly, check the status messages.

➔ The **Save** dialog opens.

4. Select a directory to which you wish to save your settings.

5. Enter a name for the *.xml file.

6. Click **Save**.

➔ The **Import/Export successful** window opens.

➔ The settings are now saved and can be called up again using the function **Load configuration**.

47

5.2   Loading SISTORE configurations

CX FDV

Prerequisite:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

Settings have been saved using the **Save configuration** function.

i | Network settings and storage media selections are not imported. This will prevent computer names and IP addresses from being assigned twice.

1.   Before loading the SISTORE configuration data, make the appropriate
     network settings and select a storage medium. See Sections 7.1 Configuring
     network settings and 11 Configuring the storage medium.
2.   In the tree view, navigate to a SISTORE device.
3.   Click **Load configuration** (see Fig. 12).
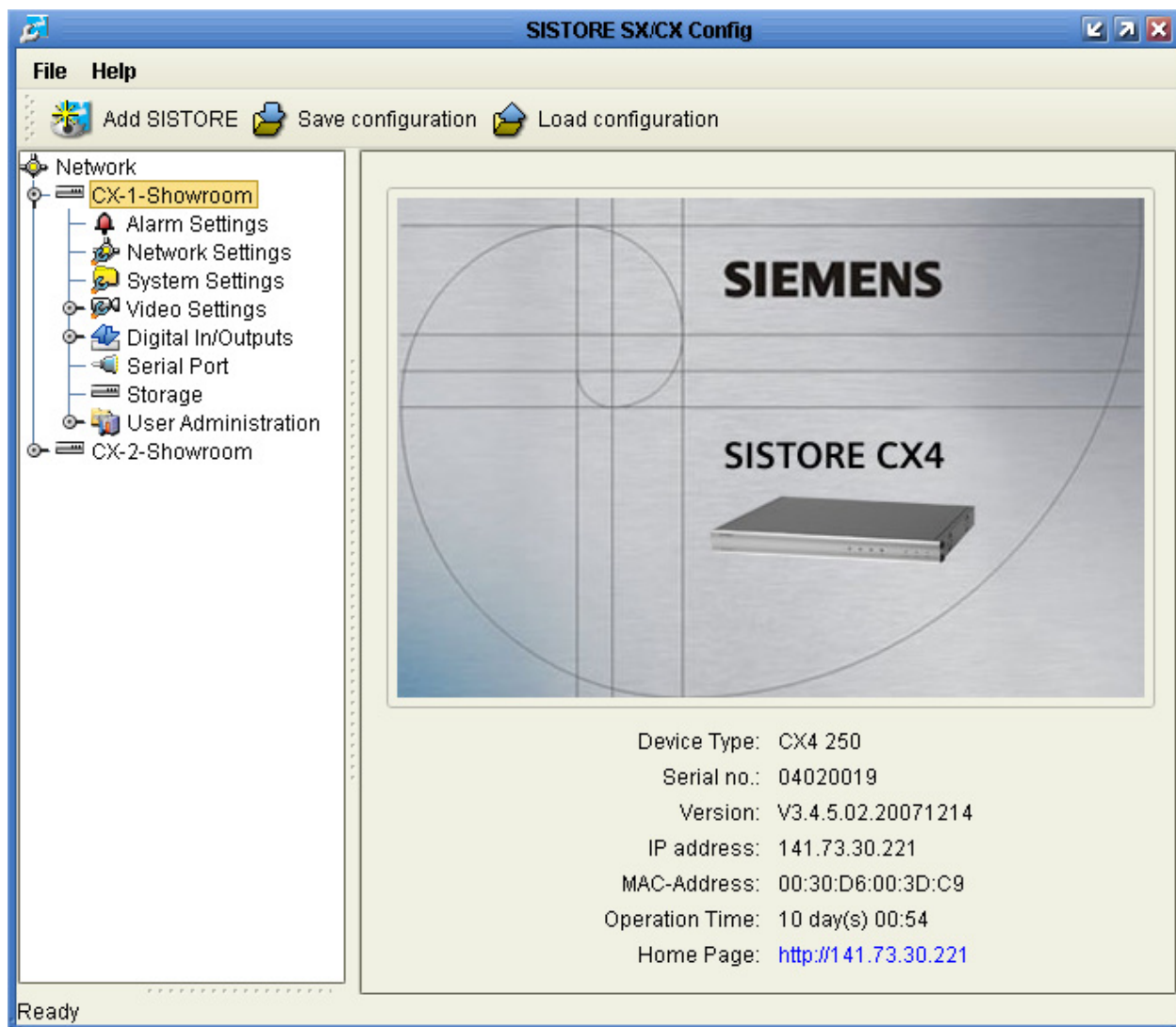   → The **Import/Export status** window opens.
     → The **Load** dialog opens.
4.   Select the configuration file you have saved
     (*.xml file or *.dvp file if the SISTORE version is lower than 3.4).
5.   Click on **Load**.
6.   Please note the output in the **Import/Export Status** window.

Output	Meaning
OK	Action was performed correctly.
Failed	Action failed.
Skipped	Action was skipped deliberately.

i | We recommend loading the SISTORE configurations once more if an action failed.

→ The device is restarted. This may take some time.
→ The **Import/Export successful** window opens.
→ The SISTORE configuration data has been loaded.

5.3   Loading FDV241 configurations

FDV

The Video Fire Controller can be configured using the configuration file 'vfc.xml'. The following FDV241 configurations will be loaded:

	Digital input	Description
Rule 1	Digital input 3 (FDnet OUT A)	Rule 1 is triggered via the FDnet and starts a recording with pre-event and post-event times.
Rule 2	Digital input 4 (FDnet OUT B)	Rule 2 enables recordings to be started and stopped by the fire alarm control panel via the FDnet.
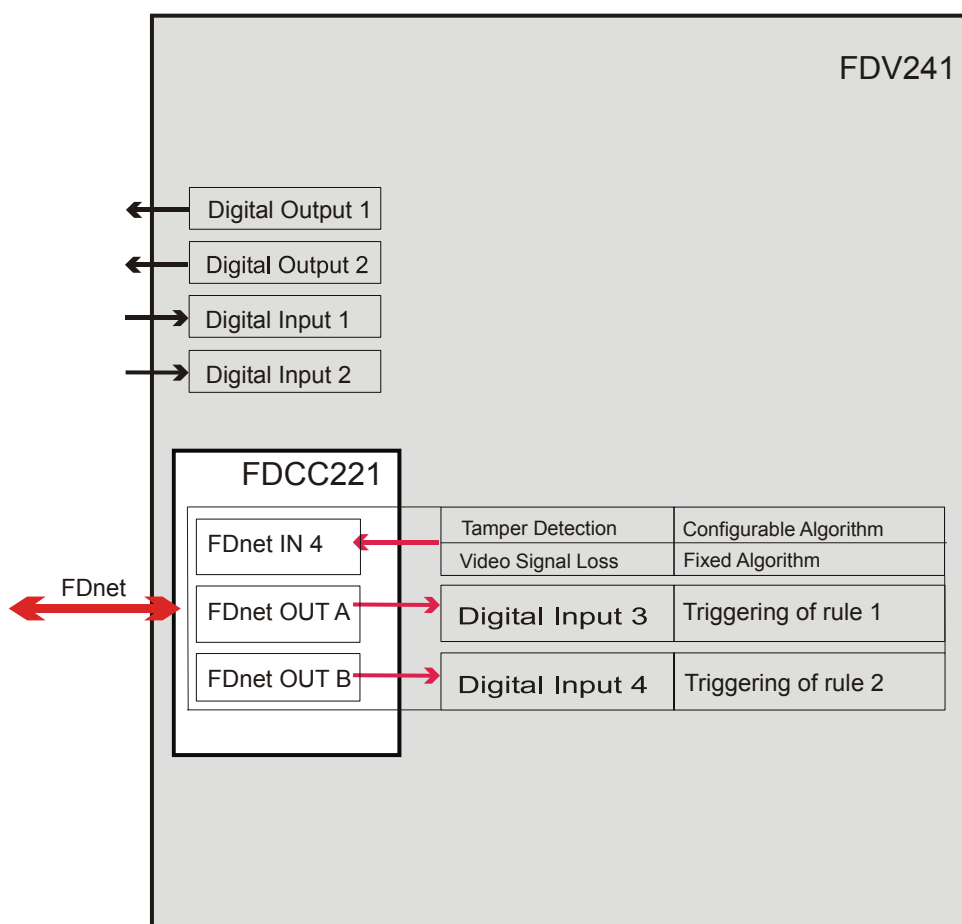
Fig. 13   Digital inputs and outputs of FDV241 – Rule configuration

ℹ️

If the tamper detection function is activated on the Video Fire Controller FDV241 (see Section: 16.5 Activating / deactivating tamper detection) and the camera is tampered with, an alarm will be reported via **FDnet IN 4** to the fire alarm control panel.

Loss of video is always reported to the fire alarm control panel, also via **FDnet IN 4**.

More detailed information on the configuration and setup of the fire alarm control panel can be found in the Configuration Manual and in the user manual for the fire alarm control panel.

Prerequisites:

A connection to the Video Fire Controller has been established. See Section: 4.1 Connecting to SISTORE device.

The controller has an integrated compact flash card. Further information on this can be found in the Startup Manuals for the Video Fire Controller.

The compact flash card is activated (see Section: 11.2 Activating a storage medium).

1. In the tree view, navigate to a Video Fire Controller.
2. Click on **Load configuration**.
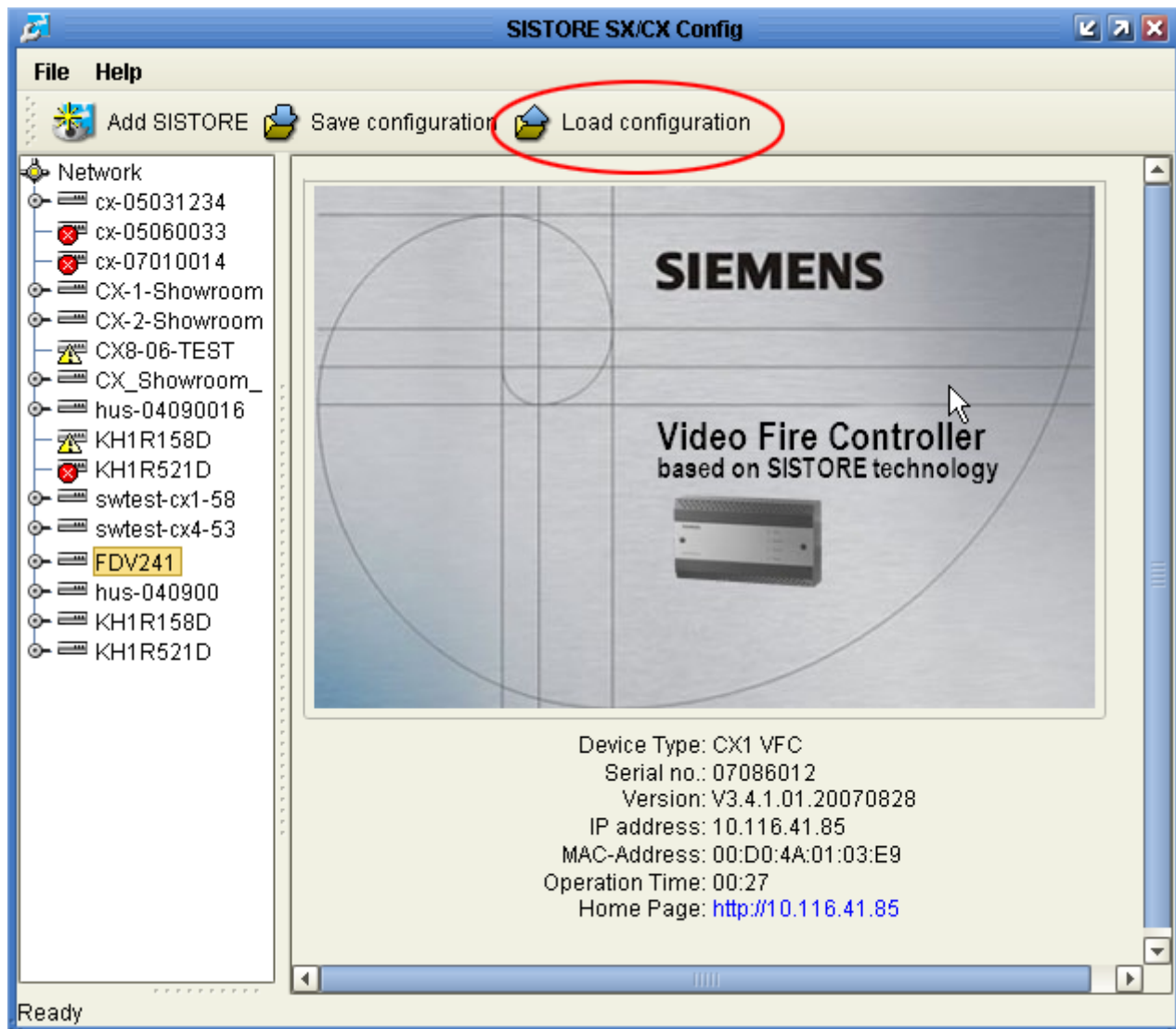
Fig. 14   FDV241 configuration data – Load configuration

➔ The **Import/Export status** window opens.
➔ The **Load** dialog opens.
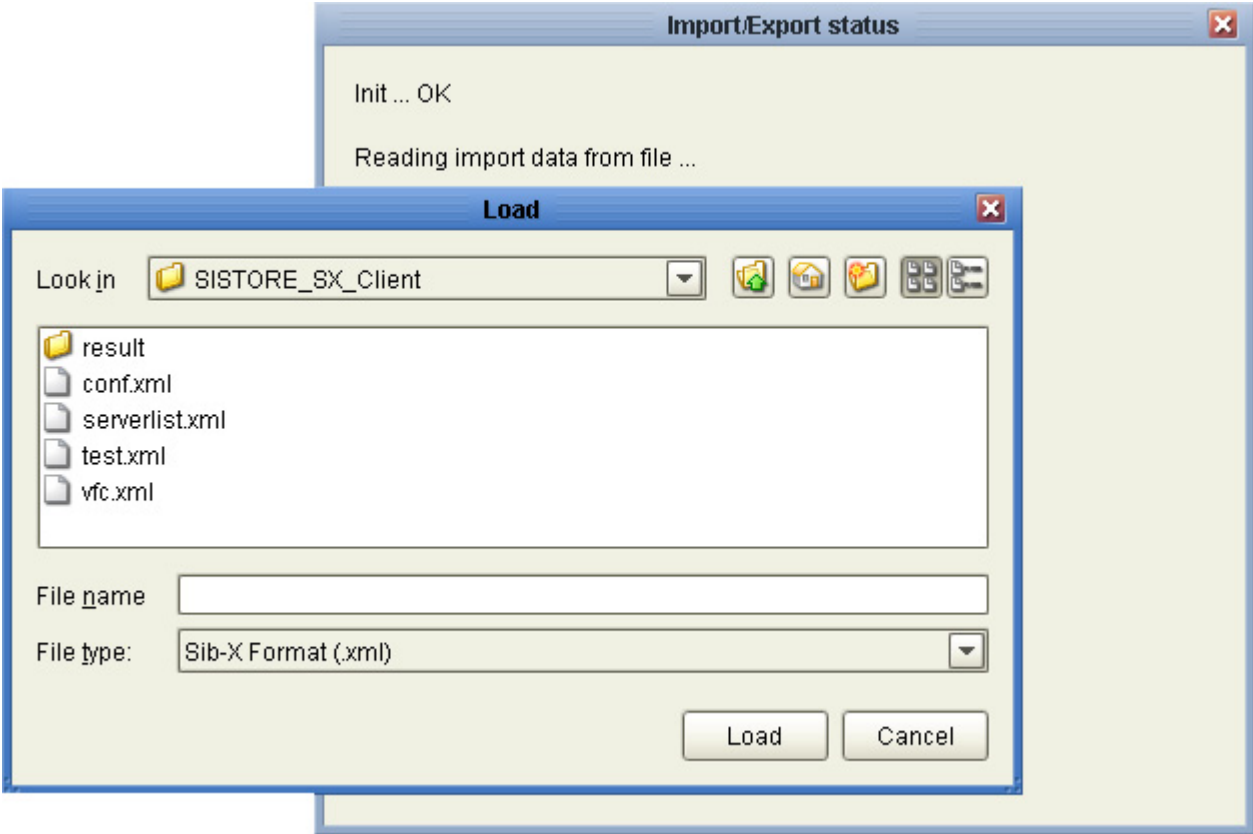
Fig. 15   Loading FDV241 configuration – Configuration file vfc.xml

3.   Select the configuration file 'vfc.xml' in the directory
          D:\CEVIS\SISTORE_SX_Client.

4.   Click on **Load**.

5.   Please note the output in the **Import/Export Status** window.

Output	Meaning
OK	Action was performed correctly.
Failed	Action failed.
Skipped	Action was skipped deliberately.

> **i**   We recommend loading the FDV241 configurations once more if an action failed.

➔ The device is started automatically. This may take some time.

➔ The **Import/Export successful** window opens.

➔ The FDV241 configuration has been loaded.

Fig. 16   SISTORE CX Client – Rule configuration

6 Alarm settings configuration

6.1 Alarm enabling

CX FDV

Alarm enabling

In the Alarm enabling tab you can define whether and how an alarm will be reported to the SISTORE Client depending on the digital inputs and detection modes. In addition to the alarm message, an alarm image can be sent.

i For the transmission of alarm images the digital inputs are assigned one-to-one to the video inputs.
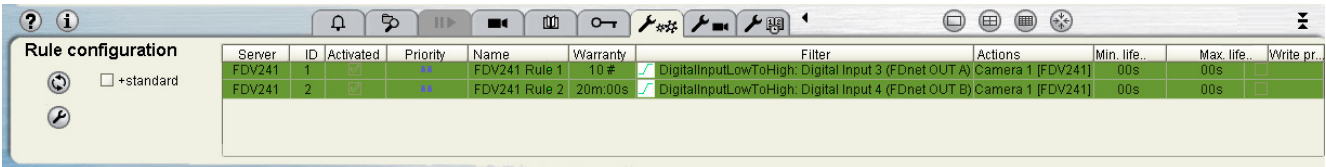Example:
When digital input **2** is triggered, the alarm image of the camera is switched to video input **2**.

Prerequisites:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

To obtain a pre-alarm picture, you must have configured pre-event recording or indefinite recording. Please also refer to the SISTORE CX Client User Manual.

To obtain an alarm picture or a post-alarm picture, you must have configured post-event recording or indefinite recording. Please also refer to the SISTORE CX Client User Manual.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Alarm settings**.
3. Select the **Alarm enabling** tab.

i The alarm image can be displayed only if a rule has been defined and a recording is available.

Fig. 17   Alarm settings – "Alarm enabling"

4.   Select the appropriate detection modes, the digital inputs and the alarm images for **Online alarms** and **Offline alarms**.

In the Online alarms section the detection modes are selected by default.

Online alarms	Offline alarms
● SISTORE CX Client is logged on	● The SISTORE CX Client is logged on but is not connected to the SISTORE device.
	● When an alarm occurs, the SISTORE CX Client is temporarily connected to the SISTORE device. In order to find the cause of the alarm, the user must log on to the SISTORE CX Client in the normal way.

5.   Either tick or untick the checkboxes for the digital inputs, the detection modes and the alarm images. See Section: 14.6.2 Definition of the alarm handling, Section: 13 Configuring motion detection, Section: 14 Configuring Enhanced Motion Detection and Section: 15 Configuring the detection of removed or left objects.

6.   Click **Apply**.

6.2 Defining alarm parameters

CX FDV

Alarm parameters

The alarm parameters define the image characteristics as well as the interval between images and the number of pre-alarm and post-alarm images.

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Alarm settings**.
3. Select the **Alarm parameter** tab.

Fig. 18   Alarm settings – "Alarm parameter" tab

4. Select an alarm filter for digital inputs.

LowToHigh	If "Low to High" is activated, a rule will be triggered when the voltage rises.
HighToLow	If "High to Low" is activated, a rule will be triggered when the voltage drops.

5. Select the appropriate **Alarm parameters** from the drop-down lists.

i	Only one pre-alarm and one post-alarm image can be displayed on the SISTORE CX Client.

Alarm parameters	Selection possibilities
Codec	JPG
Image format	QCIF, CIF, 2CIF, DCIF, 4CIF
Interval between images in sec	Defines the interval between alarm pictures (alarm picture, previous alarm and post-alarm picture) in sec.
Post alarm pictures	Besides the alarm image, up to 2 pre-alarm and post-alarm
Previous alarm pictures	images can be transmitted.

6. Click **Apply**.

6.3 Defining offline receivers

6.3.1 Defining offline clients

| CX | FDV |

Offline receivers

An offline receiver is a client which goes online when an alarm occurs so it can receive alarm messages.

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.

2. In the tree view, navigate to the node **Alarm settings**.

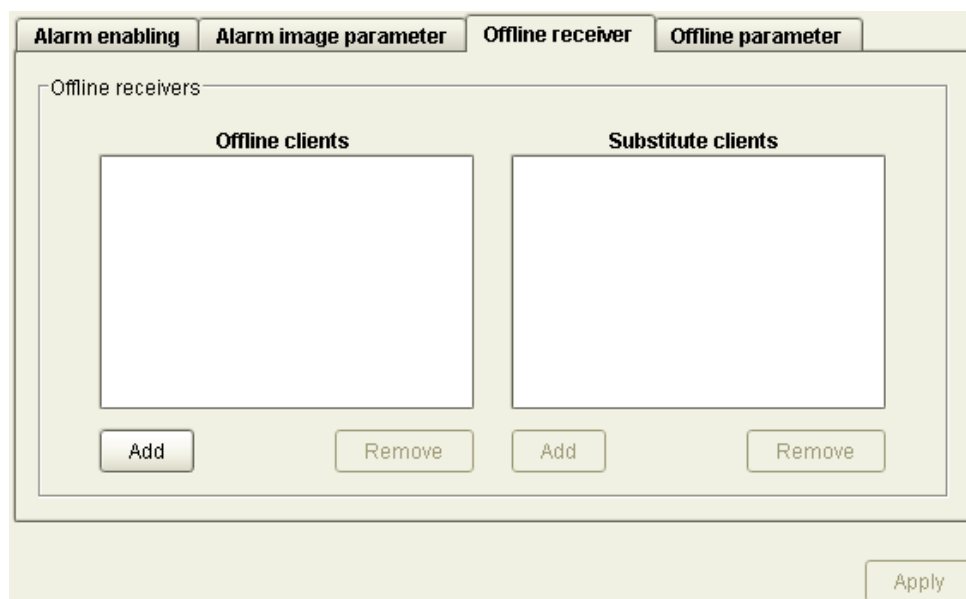**3.** Select the **Offline receiver** tab.

Fig. 19   Alarm settings – "Offline receiver"

4. Click the button **Add** below the **Offline clients** section.

55

→ The **Input IP address** dialog box opens.

5. Enter the IP address of the client PC.

6. Confirm with **OK**.

→ The client PC will be displayed in the **Offline clients** list.

7. Click **Apply**.

i	**(+2)** indicates the number of substitute clients.

6.3.2 Defining substitute clients

CX	FDV

Substitute clients

Substitute clients are clients which will be addressed in chronological order in case of a breakdown of the original client.

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.

2. In the tree view, navigate to the node **Alarm settings**.

3. Select the **Offline receiver** tab.

4. Select a client from the **Offline clients** list.

5. Click the button **Add** below the **Substitute clients** section.

→ The **Input IP address** dialog box opens.

6. Enter the IP address of the substitute client.

7. Confirm with **OK**.

→ The substitute client will be displayed in the **Substitute clients** list.

→ The number of substitute clients is displayed in addition to the client name in the **Offline-Clients** list.

6.4 Defining offline parameters

Offline parameters

Offline parameters define the connection set-up to an offline client.

i It is recommended not to change the default settings.

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Alarm settings**.
3. Select the **Offline parameter** tab.

| Alarm enabling | Alarm parameter | Offline receiver | **Offline parameter** |

Connection Establishment

Number of Retries: 2

Timeout: 10

Connection Hold Time: 15

Apply

Fig. 20   Alarm settings – "Offline parameter"

4. Select the number of attempts the system shall make to establish a connection to the offline-client in the **Number of Retries** list box.
5. Select the time in seconds after which an attempt to establish a connection to the offline client shall be interrupted in the **Timeout** list box.
6. Select the period of time in seconds for which a connection to the offline client shall be held in the **Connection Hold Time** list box.
7. Click **Apply**.
   ➔ The offline parameters are defined.

7 System settings configuration

7.1 Configuring network settings

CX FDV

Changing device names and IP settings

Prerequisite:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, open the node for the SISTORE device whose network settings you would like to configure.
3. Click **System settings** in the tree view.
4. Select the **Network settings** tab.

Fig. 21   Network settings

5. Configure the following settings in this tab:

> It is recommended to use automatic IP address assignment during setup of the SISTORE CX Config software and to manually assign a permanent IP address afterwards. This ensures that it will be possible to access the CX devices directly even in case of a failure of the DHCP server.

Network card settings	Set the network card settings correctly to match the network switch.
Assign host name	A name for the computer must be entered or changed manually in the **host name** field.

Define IP settings	• Option **Obtain an IP address automatically** enabled: The selected SISTORE CX device will be assigned an IP address automatically. If a DHCP server is provided in the network, the IP address for the SISTORE CX will be assigned by this server. If no DHCP server is provided, the SISTORE CX will generate an IP address in the address band 169.254.xxx.xxx (ZeroConf). • Option **"Obtain an IP address automatically"** disabled: The selected SISTORE CX can have the IP address, subnet mask and gateway assigned manually.

6. Click **Apply**.

7. Answer **Yes** in the confirmation dialog.

➔ The SISTORE device will be restarted.

---

i

If an IP address is changed, all references to the particular device need to be updated as well:

● Transparent data channel: Re-enter the name of the data receiver
(see Section: 10.3 Settings for transparent data channel).

● Video output configuration: Select the appropriate transmitter once more
(see Section: 8.4 Configuring video inputs).

7.2 Set date and time format

CX FDV

The display format for showing the time on video images and the time zone in which the SISTORE device operates can be defined:

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.

2. In the tree view, open the node for the SISTORE device whose date and time format you would like to change.

3. Click **System settings** in the tree view.
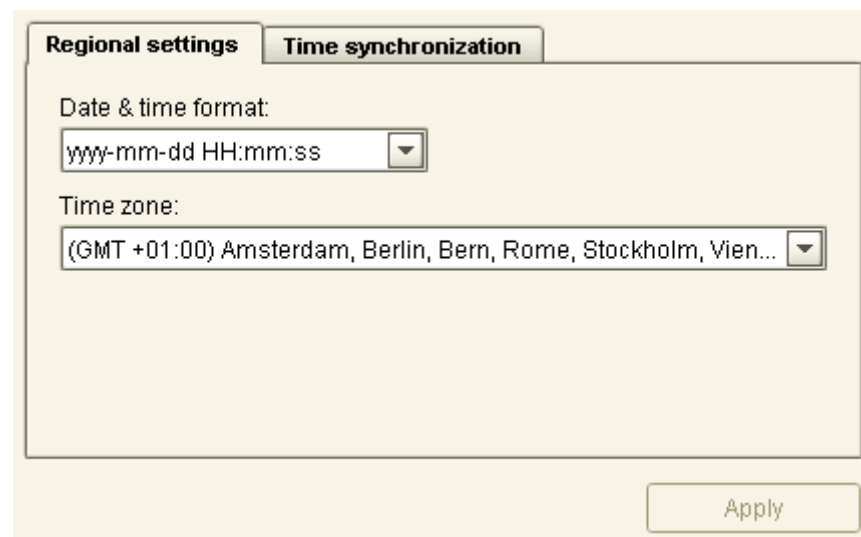
4. Select the **Regional Options** tab.

Fig. 22   "Regional settings" tab

5. Choose the desired function from the **Date & time format** dropdown list.

6. Select the time zone in which your SISTORE device operates from the **Time zone** drop-down list.

7. Click **Apply**.

SISTORE device and client PC in different time s

If the SISTORE device and the client PC are in different time zones, the recordings will always show the local time of the SISTORE device.

7.3   Synchronizing the time on SISTORE devices

CX FDV

The time on your SISTORE device can be synchronized with the time on your client PC or with the time on an NTP Server.

Prerequisite:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2.   In the tree view, navigate to a SISTORE device.
3.   Click **System settings** in the tree view.
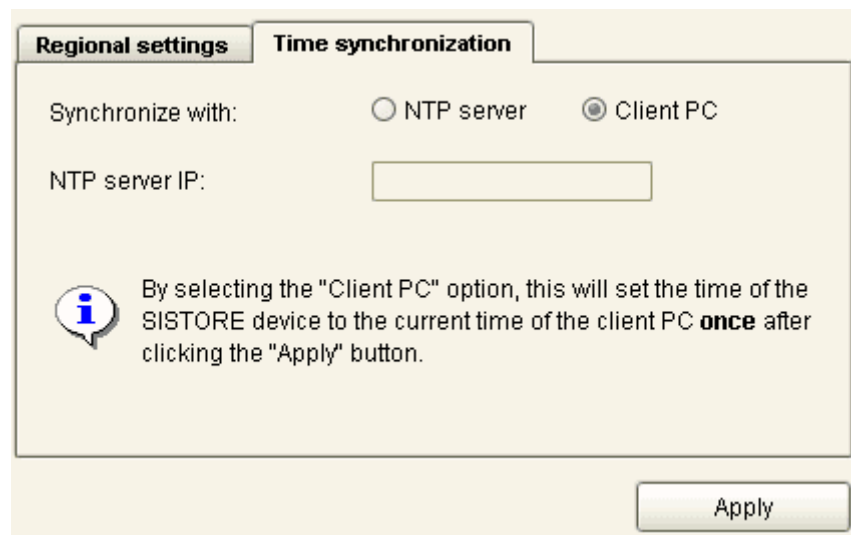4.   Select the **Time synchronization** tab.

Fig. 23   "Time synchronization" tab

5.   Select a synchronization mode:
–   Synchronize time with NTP Server:
An NTP Server always provides the current time. The time on your SISTORE device will be updated <u>continuously</u> with the time from the NTP Server. This is a periodic synchronization mode, i.e. the time is updated at regular intervals. The IP address of the NTP Server must be specified for this.
–   Synchronize time with the client PC:
The time will be synchronized <u>once</u> with the time on the client PC. This is not a periodic synchronization mode, because the time is set only once. See Section: 3.5 Set date and time of client PC and Section: 3.7 Synchronizing the time on the client PC with the time on the NTP server.
6.   Click **Apply**.

8 Video settings configuration

8.1 Set operating mode

$\boxed{\text{CX}}\boxed{\text{FDV}}$

The operating mode determines for the individual SISTORE devices how the video inputs and outputs will be used. See Section: 3.1 Operating modes and performance characteristics.

⚠	**IMPORTANT**	**Rules will be deleted** If you change the operating mode settings, all rules on the device will be deleted. The default rules will be restored automatically. ● Recreate the user-defined rules after changing the operating mode.

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, open the node for the device whose operating mode you would like to configure.
3. Click **Video settings** in the tree view.
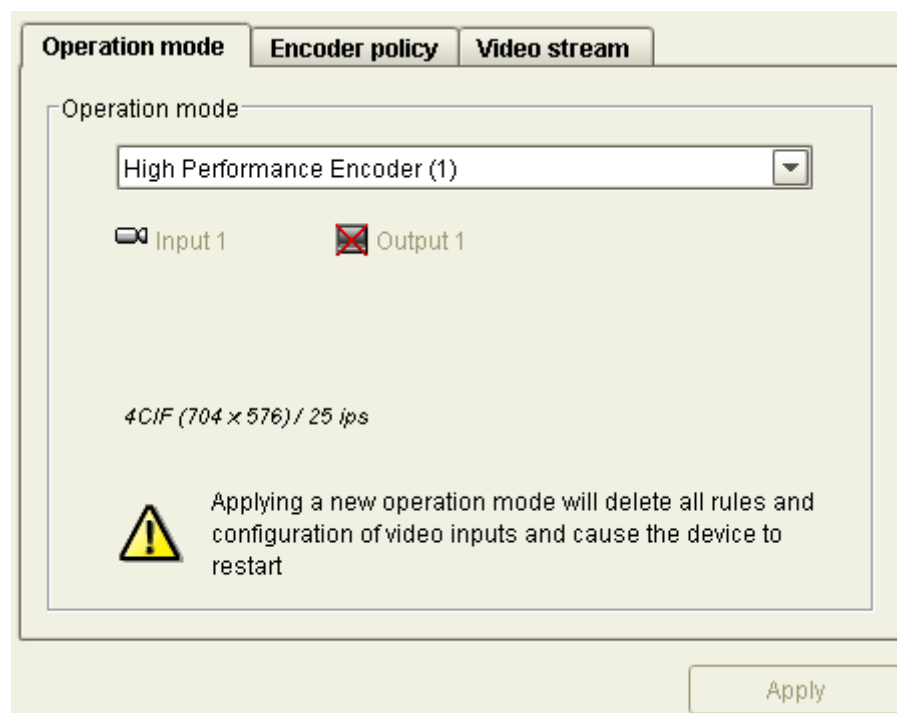4. Select the **Operation mode** tab.

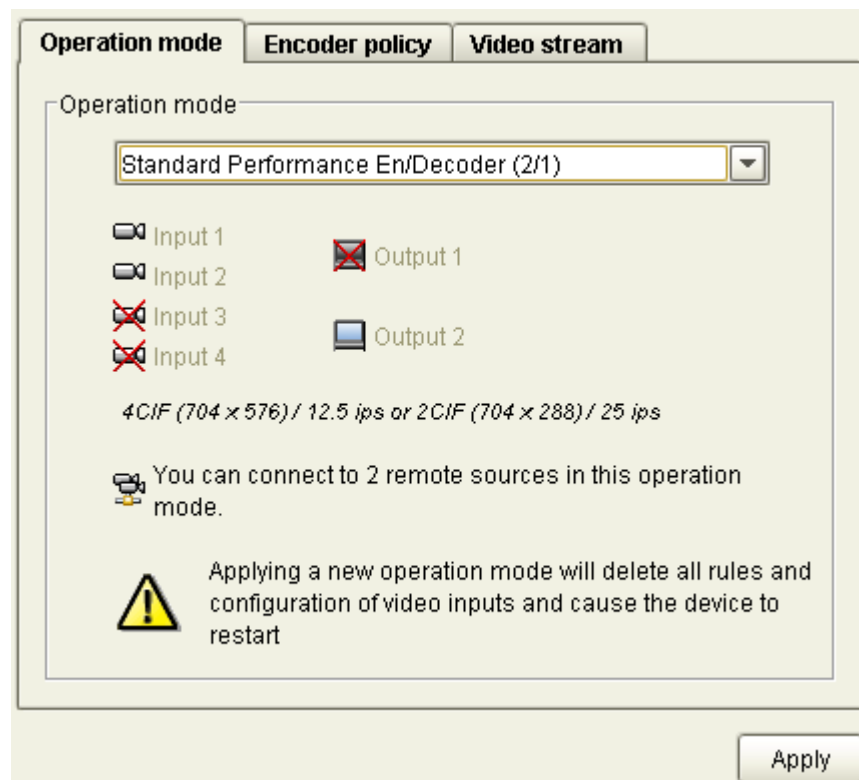Fig. 24 Video settings SISTORE CX1 – Operation mode

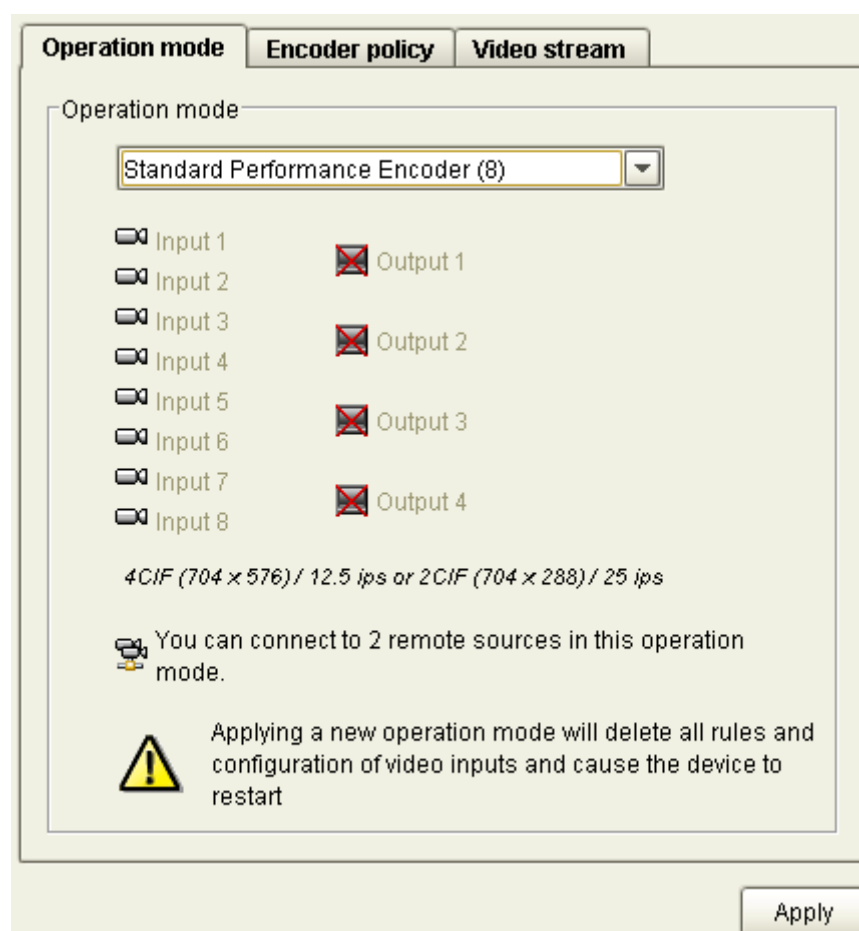Fig. 25   Video settings SISTORE CX4 – Operation mode

Fig. 26   Video settings SISTORE CX8 – Operation mode

5.   Select an operation mode from the list box.

➔ In the area below the dropdown field, you can see which video inputs and outputs are used for the particular operating mode chosen and how many remote video sources can be connected.

6. Click **Apply**.

7. Answer **Yes** in the confirmation dialog.

➔ The SISTORE device will be restarted.

➔ All rules will be deleted.

8.2   Encoder settings

8.2.1   Configuring encoder settings

CX FDV

The following encoder settings can be made:

– Encoder settings for recordings

These settings are made in the rule configuration. See Section 18 Rule configuration.

– Encoder settings for streaming

These settings are made in the streaming configuration. See Section 8.4.3 Streaming settings for video transmission .

i	In conjunction with a management system (e.g. IVM), a live video can be simultaneously requested by several clients. In that case, the settings of the client that made the last request will be applied.

8.2.2   Encoder policy

If the video is to transmitted while it is being recorded, then the encoder priority can be selected.

Prioritise encoder settings for recording	The encoder settings for recordings will be used. If no recording is taking place, the encoder policy for streaming will be applied.
Prioritise encoder settings for streaming	The encoder settings for streaming will be used. If no video is transmitted, the encoder policy for recordings will be applied.
Dual Encoding	With dual encoding, the settings for recording and streaming will not affect one another. The settings made for recording and streaming will be applied accordingly.

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the software.

2.   In the tree view, open the node for the device whose encoder policy you would like to select.

3.   Click **Video settings** in the tree view.

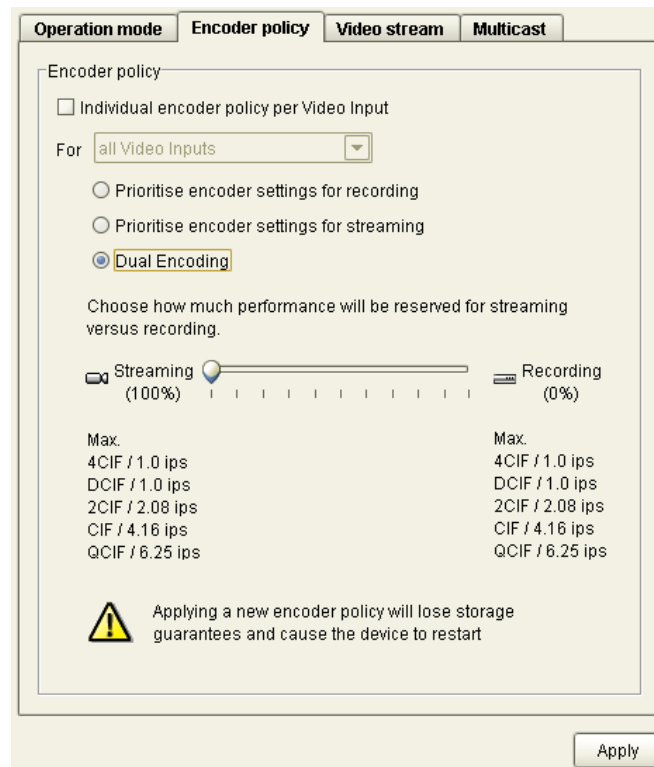4.   Select the **Encoder policy** tab.

Fig. 27   Video settings – Encoder policy

5. To apply the encoder policy to individual video inputs, mark the checkbox **Individual encoder policy per Video Input**.

– Select the individual video inputs successively and make the appropriate settings.

6. To apply the encoder policy for recordings, activate the option **Prioritise encoder settings for recording**.

7. To apply the encoder policy for streaming, activate the option **Prioritise encoder settings for streaming**.

> **i** If the option **Prioritise encoder settings for streaming** is activated, the guaranteed storage values of the rules no longer apply. Rules without guaranteed storage values are displayed with a blue background.

8. If you do not want the settings for streaming to have an effect on the settings for recording and vice versa, select the option **Dual Encoding**.

– Define the encoder performance for recording and streaming with the slide control.

➔ The maximum frame rate for each image format is displayed. See Section 24.5 Frame rate with Dual Encoding.

9. Click **Apply**.

10. Answer **Yes** in the confirmation dialog.

➔ The SISTORE device will be restarted.

➔ The selected encoder policy will be applied.

8.3   Video stream

8.3.1   Selecting codec and streaming method

CX FDV

Codecs

- MPEG-4 SVS is a video format for SIEMENS Video Streams based on the MPEG-4 technology.
- MPEG-4 SP/ASP is a video format conforming to the "International Standard ISO/IEC 14496 2 Part 2: Visual".

Visual Tools	SISTORE CX
Basic	–
– I-VOP	✓
– P-VOP	✓
– AC/DC Prediction	✓
– 4-MV, Unrestricted MV	✓
Error resilience	–
– Slice Resynchronization	✓
– Data Partitioning	–
– Reversible VLC	–
Short Header	–
B-VOP	–
Method 1/Method 2 Quantisation	–
Interlace	✓
Quarter Pel MC	–
Global Motion Compensation	–

Profile@Level
Bandwidth (KBit/s) and visual tools can be flexibly selected in the encoder.

Image format	Profile@Level
4CIF	Interlaced, max. 8000 KBit/s (implies an ASP@L5 decoder)
CIF	max. 384 KBits/s (implies a decoder conforming to SP@L3)

Streaming method

With SISTORE CX you can select among two streaming methods.

These are defined by two streaming protocols: TCP Unicast and RTP Multicast.

TCP Unicast	RTP Multicast
With this connection type, only one receiver can access an image transmitter.	Transmission of a video stream via routers/switches to several clients.

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Video settings**.
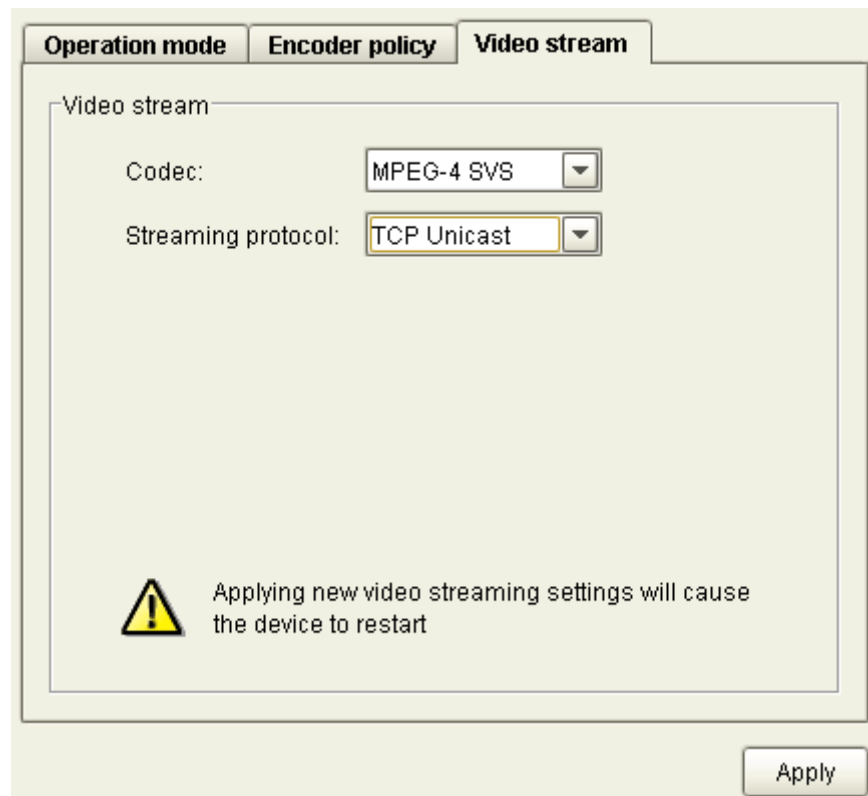**3.** Select the **Video stream** tab.

Fig. 28   Video settings – Video stream

4. Configure the appropriate settings:

Streaming method	Selection possibilities
Codec	● MPEG-4 SVS – SIEMENS Video Streams ● MPEG-4 SPASP – "International Standard ISO/IEC 14496 2 Part 2: Visual"
Streaming protocol	● TCP Unicast ● RTP Multicast ➔ The **Multicast** tab appears. See Section: 8.3.2 Configuring RTP Multicast.

5. Click **Apply**.
6. Answer **Yes** in the confirmation dialog.
   ➔ The SISTORE device will be restarted.

8.3.2 Configuring RTP Multicast

CX FDV

Prerequisite:

The streaming protocol RTP Multicast has been selected. See
Section: 8.3.1 Selecting codec and streaming method.

There are three possible ways to configure the video inputs for Multicast:

● Operation with active video inputs only

  – OR –

● Operation also with inactive video inputs

  – OR –

● Configuration of SISTORE devices lower than V3.4

Operation with active video inputs only

IMPORTANT	**Malfunction if Multicast IP addresses or ports are not unique** Multicast will not work in very large systems using switches with IGMP snooping. Multicast IP addresses must differ in one place. Multicast ports must differ in two places. ● Make sure to always assign unique combinations of multicast IP addresses and ports.

1. Select the **Multicast** tab.

Fig. 29   Video settings – Multicast

2. Enter a multicast IP address and a multicast port for each video input.

   – OR –

   In order to assign the same multicast IP address and multicast port to all video inputs, click on the button **=**.

   – OR –

   In order to automatically assign consecutive multicast IP addresses and ports, click on the button **+**.

3. To activate the RealTime Control Protocol (RTCP), mark the checkbox **Enable RTCP check**.

4. Click **Apply**.

5. Answer **Yes** in the confirmation dialog.

   → The SISTORE device will be restarted.

Operation also with inactive video inputs

[**i**]   The inactive video inputs are assigned dummy multicast IP addresses and ports.

1. Assign an dummy multicast IP address and a dummy multicast port during setup. See Section: 8.3.3 Configuring dummy multicast IP address and port.

2. Select the **Multicast** tab.

Fig. 30   Multicast – Inactive video inputs

3. Enter a multicast IP address and a multicast port for each video input.

   – OR –

In order to assign the same multicast IP address and multicast port to all video inputs, click on the button **=**.

– OR –

In order to automatically assign consecutive multicast IP addresses and ports, click on the button **+**.

4. To activate the RealTime Control Protocol (RTCP), mark the checkbox **Enable RTCP check**.

5. Click **Apply**.

6. Answer **Yes** in the confirmation dialog.

→ The SISTORE device will be restarted.

Configuration of SISTORE devices lower than V3.4

1. Select the **Multicast** tab.

Fig. 31 Multicast – SISTORE device lower than V3.4

2. Enter a multicast IP address and a multicast port for the first video input.

→ All video inputs are assigned the same multicast IP address.

→ The other video inputs are automatically assigned consecutive multicast ports.

3. Click **Apply**.

4. Answer **Yes** in the confirmation dialog.

→ The SISTORE device will be restarted.

8.3.3   Configuring dummy multicast IP address and port

CX FDV

i

- The inactive video inputs are assigned dummy multicast IP addresses and ports.
- We recommend configuring the dummy multicast IP address and the dummy multicast port during initial setup as it will be more cumbersome to do it at a later date.

The default multicast IP address and the default multicast port are as follows: 239.254.254.254:34567

1.   Right-click on the desktop icon of the SISTORE Config application.

2.   Select **Properties**.

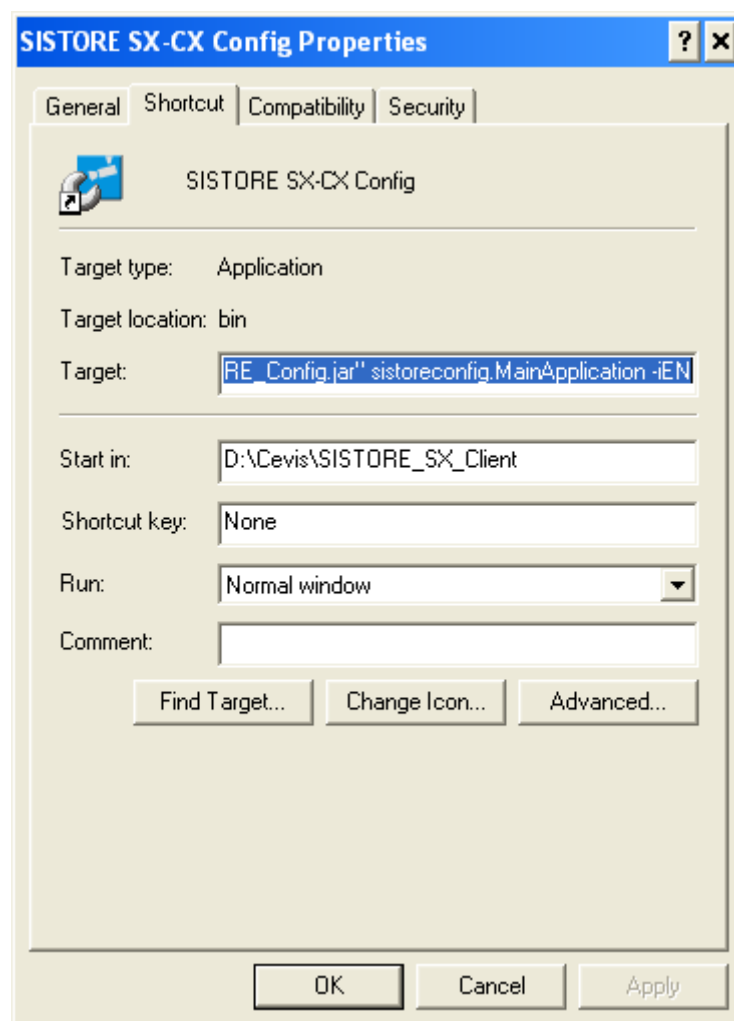➔ The following dialog box opens.

Fig. 32   SISTORE CX Config - Properties

3.   Select the **Shortcut** tab.

4.   Enter the following command line parameter containing the desired multicast IP address and the multicast port in the **Target** box:
     -mcDummy=xxx.xxx.xxx.xxx:yyyyy

5.   Click **OK**.

8.4 Configuring video inputs

CX FDV

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

An operating mode that supports video inputs has been chosen. See Section: 8.1 Set operating mode.

> **i** Access to this function can be limited with the user administration functions. See Section: 12 User administration and administration of rights.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, open the node for the SISTORE device whose video input you would like to configure.
3. Open the node **Video settings**.
   → The tree view will now show the video inputs of the SISTORE device.
4. Now select the **video input** that you want to configure.
   → If a live video is being transmitted to this video input, it will be displayed below the tree structure.

Fig. 33   Video settings – Live video

Button functions for live video display

 Start playback

 Stop replay

The following information is found in the video input configuration:

Server	Recording computer
Camera	Camera names, can be changed (max. 50 character long)
Input	Video input
Pre-event recording time	Recording duration prior to an event being triggered
Pre-event image rate	Image rate
Pre-event image format	Image format in QCIF, CIF, 2CIF, DCIF or 4CIF
Pre-event image quality	Image quality. See Section: 24.4 SISTORE CX network utilization and recording times.
Default image rate	Image rate in frames per second
Default image format	Image format in QCIF, CIF, 2CIF, DCIF or 4CIF. See Section: 24.2 Supported image formats.
Default image quality	Compression parameters
Default priority	Priority factor in case of resource conflicts

8.4.1　Configuring video parameters

CX FDV

1. In the tree view, navigate to the node representing the video input of the camera whose video parameters you want to configure. See Section: 8.4 Configuring video inputs.

2. Select the **Video parameters** tab.

Fig. 34　Video settings – Video parameters

3. Set the values for brightness, contrast, colour saturation and sharpness using the slide controls. The settings can be checked immediately with the live video signal.

4. Mark the checkbox for **Automatic brightness control** as required.

5. Click **Apply**.

6. Click **Default settings** to restore the default settings.

8.4.2   Configuring text overlay

CX FDV

1.   In the tree view, navigate to the node representing a video input. See Section: 8.4 Configuring video inputs.

2.   Select the **Text overlay** tab.

Fig. 35   Video settings – Text overlay

i	Maximum number of characters: 32 characters
	You can only use ISO-8859-1 (Latin-1) characters.
	(Characters used in Western European and American languages)

3.   Enter some text in the text field.

4.   To overlay the text on the video image, mark the checkbox **Overlay text**.

1.   Set the X/Y coordinates of the text in pixels.

      x=0 ; y=0   text overlay = top, left
      X=704 ; y=288   text overlay = bottom, right

2.   To overlay the date and time on the video image, mark the checkbox **Overlay time**.

3.   Set the X/Y coordinates of the text in pixels.

4.   Click on the **Text color** button.

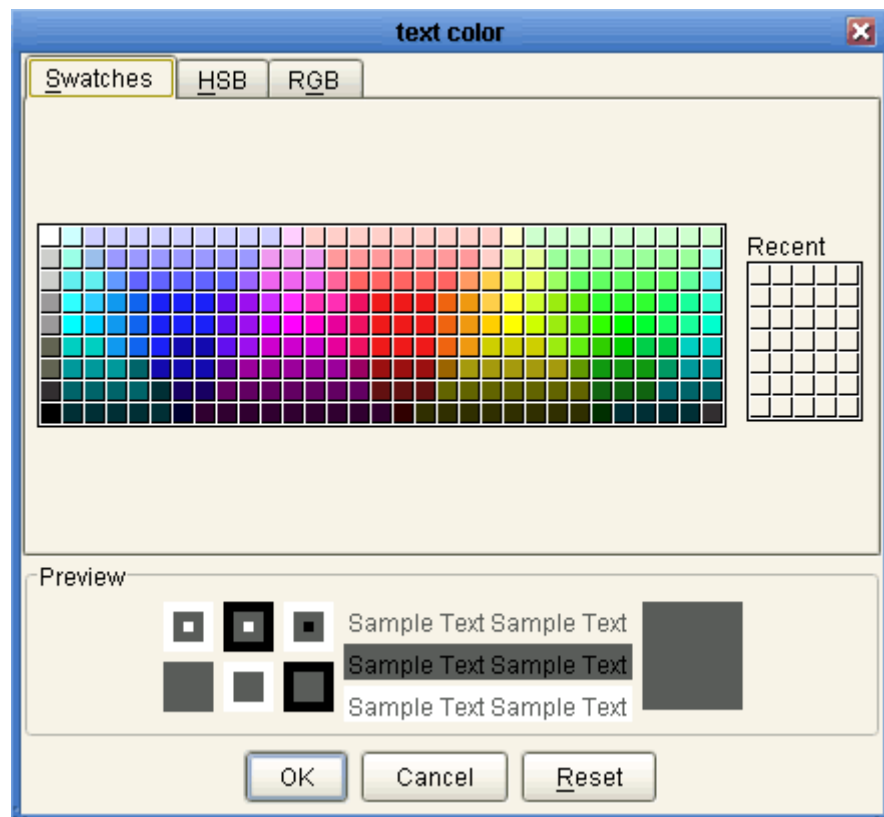➔ The **Text color** dialog box opens.

Fig. 36   "Text color" dialog box

1.   Select a colour.

2.   Click **OK**.

3.   Click **Apply**.

Video settings configuration

8.4.3   Streaming settings for video transmission

CX FDV

1. In the tree view, navigate to the node representing the video input of the camera whose streaming settings you want to configure. See Section: 8.4 Configuring video inputs.

2. Select the **Streaming** tab.

Fig. 37   Video settings – Streaming

3. Use the dropdown fields to select the following settings:
    – Image rate
    – Resolution
    – Quality
    ➔ If no recording is running on this video input the settings can be checked in the status bar of SISTORE CX Config.

    The field **Network usage** shows the network load that would result from these settings. See Section: 24.4 SISTORE CX network utilization and recording times.

4. Click **Apply**.

8.4.4 Activating/deactivating camera control functions

CX FDV

Prerequisite:

The serial interface operates in telemetry server mode. See Section: 10.1 Serial port operation modes.

1. In the tree view, navigate to the node representing the video input of the camera whose control functions you want to activate/deactivate. See Section: 8.4 Configuring video inputs.

2. Select the **PTZ** tab.

Pre-event recording		Manual recording parameters		
Video parameters	Text overlay	Streaming	Change Name	PTZ

PTZ

☐ PTZ control enabled

☐ Variable Speed

Address: 1 ▼

Camera Type: ▼

Apply

Fig. 38 Video settings – "PTZ"

3. Click **Apply**.
4. Activate the camera control functions for the desired video input.

8.4.5   Renaming video inputs

CX FDV

1. In the tree view, navigate to the node representing the video input of the camera whose control functions you want to activate/deactivate. See Section: 8.4 Configuring video inputs.

2. Select the **Change Name** tab.

Fig. 39   Video settings – "Change Name"

i   The name of the video input can be up to 50 characters long.

3. Enter the name of the video input in the **Name** field.
    ➜ This will make it easier to identify the video input.

4. Click **Apply**.

8.4.6   Pre-event parameters

CX FDV

| **i** | Pre-event parameters apply per video input for all rules. |

1. In the tree view, navigate to the node representing the video input of the camera whose control functions you want to activate/deactivate. See Section: 8.4 Configuring video inputs.

2. Select the **Pre-event recording** tab.

Fig. 40   Video settings – "Pre-event recording"

3. Use the dropdown fields to select the following settings:

| **Pre-event recording time** | A recording with pre-event time is an endless loop. When an event occurs (such as a hold-up event), the history prior to the event can be seen with a search. The defined pre-event time is guaranteed to be retained. The minimum pre-event time (ring buffer) is 10 seconds, the maximum can be up to 6 hours. |

Image rate	Depends on the operating mode. See Section: 3.1 Operating modes and performance characteristics.
Image format	Depends on the operating mode. See Section: See Section: 3.1 Operating modes and performance characteristics.
Image quality	Lowest image quality
	Low image quality
	Default image quality
	High image quality
	Highest image quality

ⓘ When configuring a remote video source (e.g. IP camera) the image rate, image format and image quality can only be changed via the homepage of the remote video source. See Section: 8.6 Configuring remote video sources.

4. Click **Apply**.

8.4.7 Parameters for manual recordings

CX **FDV**

ⓘ **NOTE**
- The parameters for manual recordings apply only if other values are not set by rules.
- The parameter settings options affect the pre-event recording.

1. In the tree view, navigate to the node representing the video input of the camera whose control functions you want to activate/deactivate. See Section: 8.4 Configuring video inputs.
2. Select the **Manual recording parameters** tab.

| Video parameters | Text overlay | Streaming | Change Name |
| Pre-event recording | | Manual recording parameters | |

Manual recording parameters

Priority	Normal
Image rate	6.25
Image format	CIF
Image quality	Standard image quality

Apply

Fig. 41   Video settings – "Manual recording parameters"

3. Use the dropdown fields to select the following settings:

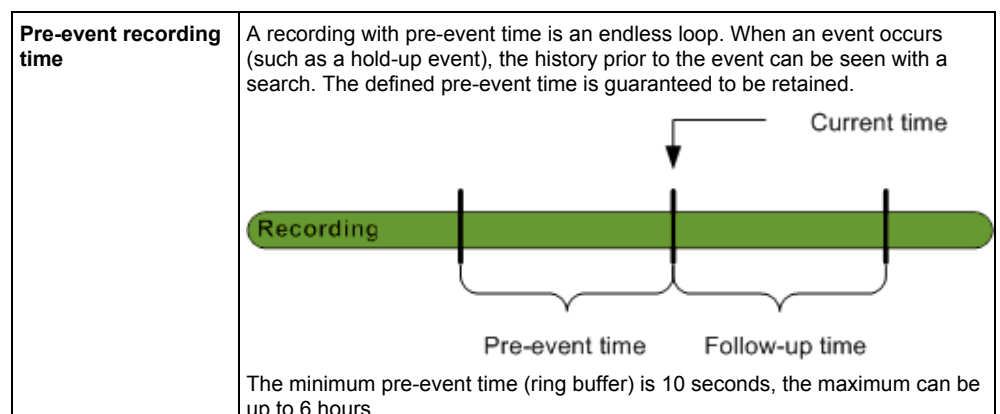|	
Priority	Low
	Normal
	High
	High, low resolution
Image rate	The image rate depends on the operating mode. See Section: 3.1 Operating modes and performance characteristics.
Image format	The image format depends on the operating mode. See Section: 3.1 Operating modes and performance characteristics.
Image quality	Lowest image quality
	Low image quality
	Default image quality
	High image quality
	Highest image quality

> **i** When configuring a remote video source (e.g. IP camera) the image rate, image format and image quality can only be changed via the homepage of the remote video source. See Section: 8.6 Configuring remote video sources.

4. Click **Apply**.

8.5   Configuring video outputs

CX FDV

A SISTORE device (= analog monitor) can have the video input (= camera or signal) of another SISTORE device connected to its video output (in addition to or alternative to the usual connection of an analog monitor), so that the output of one device is sent automatically to the video input of the second device.

Prerequisites:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

An operating mode that supports video inputs has been chosen. See Section: 8.1 Set operating mode.

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the software.

2.   In the tree view, open the node for the SISTORE device whose video output you would like to configure.

3.   In the tree view, open the node **Video settings**.

➔ The tree view will now show the video outputs of the SISTORE device.

4.   Now select the **video output** in the tree that you want to configure.

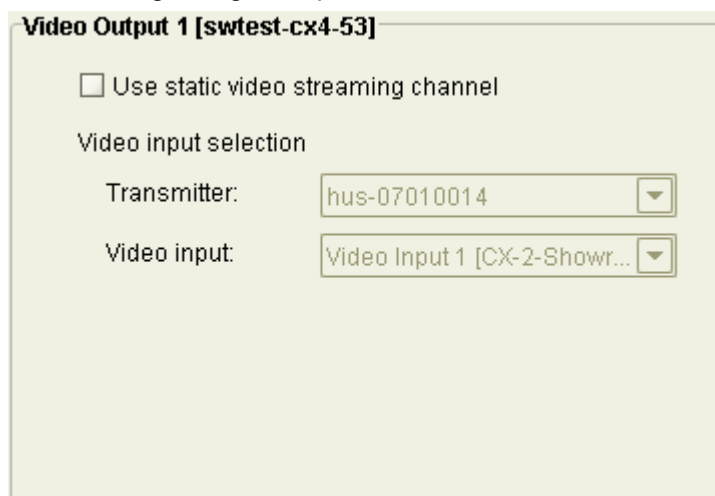➔ The following dialog box opens:

Fig. 42   "Video output" dialog box

5.   Select or deselect the checkbox **Use static video streaming channel**.

6.   Select the SISTORE device sending the data and the desired video input from the dropdown lists.

7. Click **Apply**.

→ The configuration parameters that were set will be displayed. The current state of the configuration (streaming details) can be checked on the SISTORE CX client. Further information on this can be found in the SISTORE CX Client User Manual.

→ The video output has been configured.

i	The settings for the static video streaming channel can also be changed with the following applications: ● SISTORE CX Client: By dragging and dropping cameras to monitors ● IVM: By dragging and dropping cameras to monitors

8.6 Configuring remote video sources

CX FDV

Remote video sources (e.g. IP cameras) are not directly connected to the device; the video data from the remote video sources are transmitted via Ethernet.

Depending on the SISTORE device and the selected mode of operation, up to 4 remote video sources can be configured in SISTORE CX Config. See Section: 3.1Operating modes and performance characteristics.

i	Please take into account that SISTORE CX Config V3.5 supports only hybrid MPEG4 IP cameras of type CCIC1345-LP, CCIS1345-LP and CCIW1345-LP.

Prerequisites:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

An operating mode that supports remote video sources has been chosen. See Section: 8.1 Set operating mode.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, open the node for the SISTORE device whose remote video sources you would like to connect.
3. Click the **Video settings** node.

→ The IP cameras are displayed in a table.

4. In the tree view, open the node **Video settings**.

→ Between 1 and 4 dummy IP cameras will be displayed depending on the operation mode.

5. Select an IP camera.

➔ The following dialog box opens:

Fig. 43   Video settings – Remote video sources

6.   Select a camera type in the **Type** list box.

7.   Enter a camera name in the **Name** text field.

8.   Enter the IP address of the remote source in the **IP Address** input field.

– OR –

Click the button […] **Discover remote video source…** and select a remote video source.

9.   To configure the remote video source, click on the blue link.

➔ The homepage of the remote video source is opened.

	Risk of software malfunction
	If a remote video source is not configure correctly, malfunctioning may result. Therefore carry out the following steps:
	1. Make sure that no recording is in progress.
IMPORTANT	**2.** Select "MPEG4" as the streaming protocol on the homepage of the remote video source. Further information on this can be found in the Startup Manuals for the remote video sources.
	3. Activate the NTP Server on the homepage of the remote video source. Further information on this can be found in the Startup Manuals for the remote video sources.

10.   Configure the pre-event recording time and the priority for the manual recording parameters on the corresponding tabs. See Section 8.4.6 Pre-event parameters and Section 8.4.7 Parameters for manual recordings.

11.   Configure additional parameters via the home page of the unit.

12.   Click **Apply**.

8.6.1 Deleting remote video sources

1. Proceed as described in Section 8.6 Configuring remote video sources.
2. Delete the IP address in the **IP address** text field.
3. Click **Apply**.

9 Configuring digital inputs and outputs

> **i** The digital inputs and outputs of the Video Fire Controllers FDV241 are configured using the configuration file **vfc.xml** (see Section: 5.3 Loading FDV241 configurations).

9.1 Selecting digital inputs and outputs

CX FDV

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
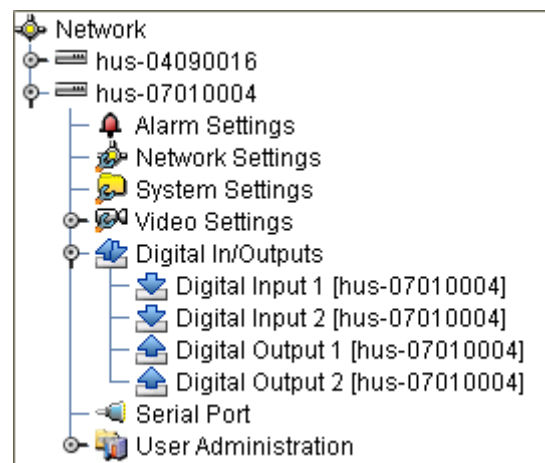

Fig. 44   Digital inputs and outputs

2. Navigate to the node **Digital In/Outputs**.

9.2 Overview digital inputs and outputs

CX FDV

Overview Digital Inputs and Outputs

Digital Inputs and Outputs	Name
Digital Input 1	Digital Input 1 [hus-07010004]
Digital Input 2	Digital Input 2 [hus-07010004]
Digital Output 1	Digital Output 1 [hus-07010004]
Digital Output 2	Digital Output 2 [hus-07010004]

Fig. 45   Overview digital inputs and outputs

1. In the tree view, navigate to the node **Digital In/Outputs**.

9.3 Renaming digital inputs and outputs

CX FDV

Change Name

Digital Input   Digital Input 2

Name   Digital Input 2 [CX_Showroom_mon]

Apply

Fig. 46   Digital inputs and outputs – Change Name

1. Select a digital input or output in the tree structure.
2. Enter a name in the **Name** field.
3. Click **Apply**.

9.4 Changing digital output parameters

CX FDV

Fig. 47 Digital outputs – Change parameter

1. Select a digital output in the tree structure.
2. Enter a name in the **Name** field.
3. Select either **Opener (n/c)** or **Closer (n/o)**.

Opener n/c (normally closed)	**The output is normally closed and will be opened when an alarm occurs.**
Closer n/o (normally open)	The output is normally open and will be closed when an alarm occurs.

4. Activate either **Internal**, **External** or **Error**.

Internal	**The output is triggered by the "Enhanced Motion Detection" or the "Detection of removed or left objects" function.**
External	The output is triggered via an external client, e.g. IVM
Error	The following malfunctions are indicated on the SISTORE device: ● Hard disk failure ● SISTORE server failure ● Loss of video signal

5. Click **Apply**.

10 Serial port configuration

10.1 Serial port operation modes

CX FDV

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Serial Port**.
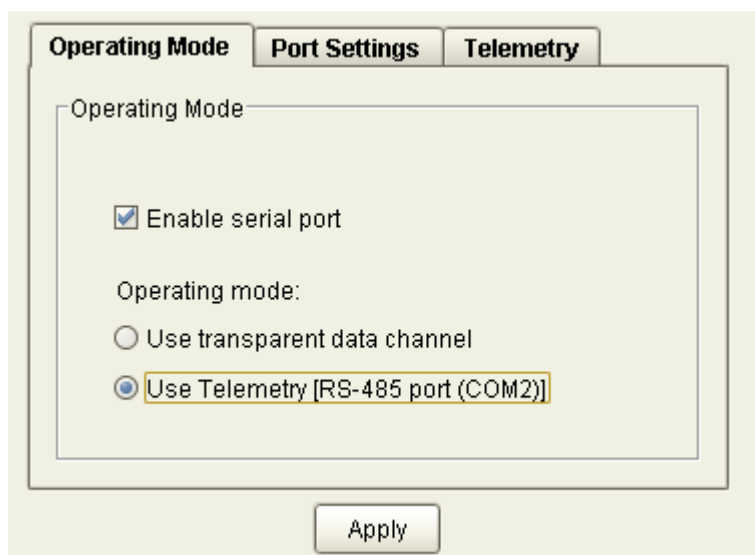3. Select the **Operation mode** tab.

Fig. 48   Serial port – "Operation Mode"

4. Select an operation mode for the serial port.
5. Select the "Enable serial port" check box.
6. Click **Apply**.

Siemens Building Technologies
Fire Safety & Security Products

Operation mode "Transparent data channel"

i	**NOTE** The transparent data channel is not always transparent, i.e. a reliable performance cannot be guaranteed with all kinds of devices. For instance, 9-bit protocols are not supported. RS-485 supports only protocols which transmit reply telegrams with a delay of at least 10 ms. The transmission latencies of the telegrams may differ significantly depending on the utilization of the SISTORE CX units and the network; as a result, protocols that expect short response times will not work properly.

It is possible to set up a transparent data channel between two SISTORE devices. The RS485 cables of cameras with pan/tilt head (domes) can thus be "extended" to the control unit. The two SISTORE devices represent the transmitting and the receiving station:

Transmitter	The SISTORE CX that is transmitting RS232 data (e.g. control panel, joystick)
Receiver	The SISTORE CX that is receiving RS232 data (e.g. Dome)

See Section: 10.3 Settings for transparent data channel.

Operation mode "Telemetry"

If the "Telemetry" operation mode is set, Domes and PTZ cameras can be controlled.

The integrated telemetry server provides the following functions:

- PTZ
- Moving cameras to predefined positions and saving positions
- Camera/Dome OSD control
- Variable speed control

i	When you have set the operation mode "Telemetry", the camera control functions must be activated/deactivated for the desired video inputs. Afterwards the PTZ control function is available on the SISTORE CX client. See Section: 8.4.4 Activating/deactivating camera control functions.

See Section: 10.4 Protocol for camera control.

10.2   Serial port settings

CX FDV

Prerequisite:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the
      software.
2.   In the tree view, navigate to the node **Serial Port**.
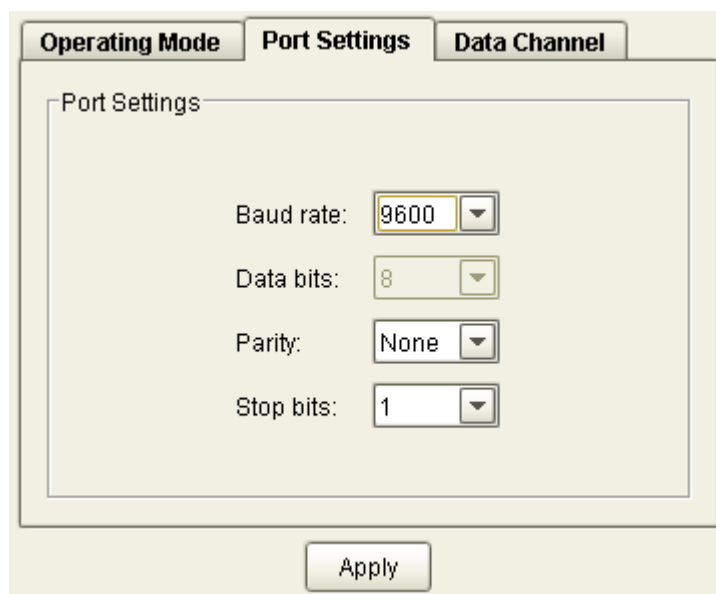3.   Select the **Port settings** tab.

Fig. 49   Serial port – "Port Settings"

4.   Configure the following settings in this tab:

Baud rate:	19200
Data bits:	8
Parity:	none
Stop bits:	1

5.   Click **Apply**.

10.3   Settings for transparent data channel

CX FDV

Prerequisite:

The operation mode "Transparent data channel" has been set for the serial port.
See Section: 10.1 Serial port operation modes.

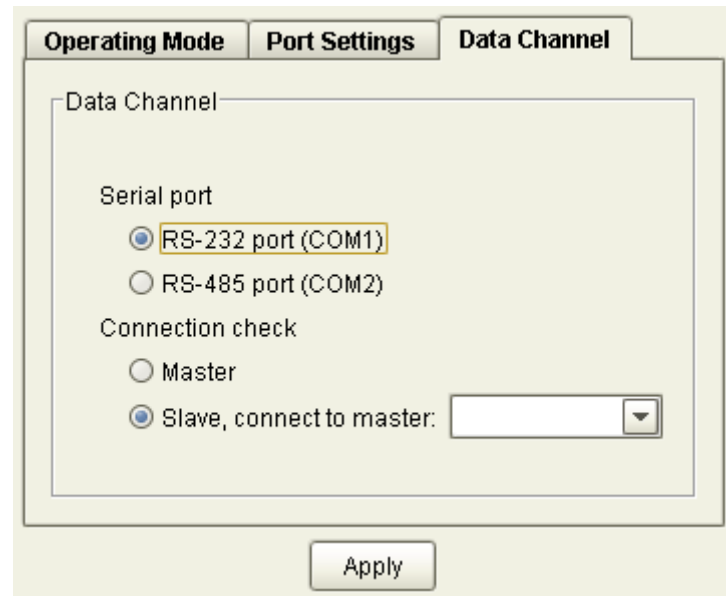**1.**   Select the **Data Channel** tab.

Fig. 50   Serial port – SISTORE CX4

i   On SISTORE CX8 the serial port is set by default.

2.   Select the serial port.
3.   Choose whether the device is to be used as a data receiver (slave) or a data
transmitter (master).
4.   If the device is used as a slave, the master must be selected additionally from
the drop-down list.
5.   Click **Apply**.

10.4   Protocol for camera control

CX FDV

Prerequisite:

The operation mode "Transparent data channel" has been set. See Section: 10.1 Serial port operation modes.
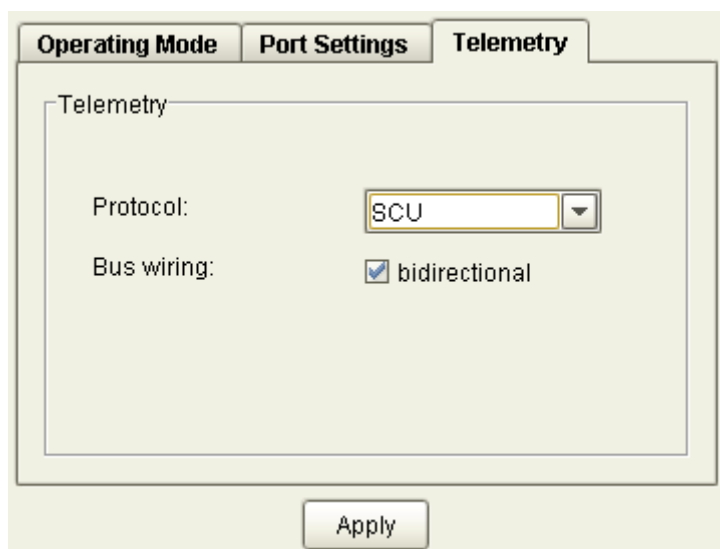
1.   Select the **Telemetry** tab.

| Operating Mode | Port Settings | **Telemetry** |

Telemetry

Protocol: SCU ▾

Bus wiring: ☑ bidirectional

Apply

Fig. 51   Serial port – Telemetrie

2.   Select the appropriate protocol for camera control from the drop-down list.
You can choose from the following protocols:

SCU protocol
CCDA protocol
PELCO-D protocol
PANASONIC protocol
MOLYNX protocol
LEDERER protocol

3.   Click **Apply**.

11 Configuring the storage medium

11.1 Displaying storage medium and storage capacity

| CX | FDV |

> The storage capacity is displayed as a static value which is updated only when the node **Storage** is opened..

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Storage**.
3. Select the **General** tab.
    → The selected storage medium of the SISTORE device, its status and description, as well as its storage capacity are displayed.
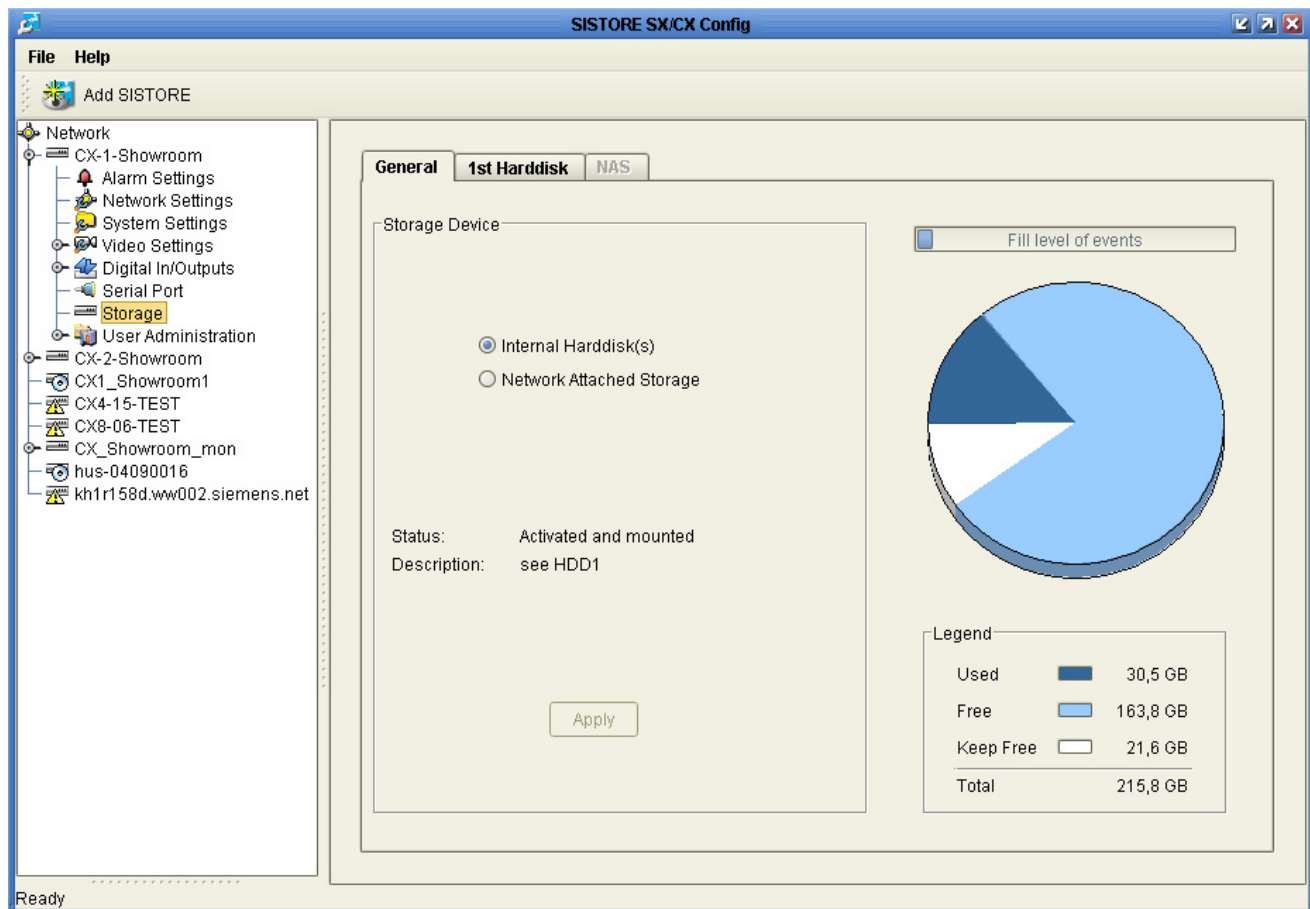

Fig. 52   Video Storage – Storage capacity

11.2   Activating a storage medium

CX FDV

| **i** | The storage medium **Internal HD** is set as default. |

The following additional storage media are available depending on the SISTORE device:

- Internal hard disk mirror (RAID-1)
- Internal compact flash
- Network-attached storage
- External SCSI device

| ⚠ | **IMPORTANT** | **Data loss due to hard disk formatting**
When a storage medium is activated, the hard disk is always formatted. During this process all data is deleted.
• Make sure that no data is lost.
• Always format the hard disks during initial start-up. |

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Storage**.
3. Select the **General** tab.
4. Select a storage medium by activating the appropriate option (see Fig. 52).
5. Click **Apply**.
6. Answer **Yes** in the confirmation dialog.
   ➜ The SISTORE device is formatted and then restarted.
7. Log on to the SISTORE device again.
   ➜ The storage medium **Internal HDD** is deactivated.
   ➜ The new storage medium is activated.

11.3 Displaying status information on the internal hard drives

CX

Prerequisites:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

The internal hard drives have been installed.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Storage**.
3. To display the status information of the first or second internal hard drive, select the corresponding tab **HDD1** or **HDD2**.
   → The status information of the corresponding internal hard drive will be displayed.

Fig. 53   HDD 1 – Status information

11.4   Mirroring internal hard disks

CX

Prerequisites:

The SISTORE device has two internal hard drives. See Section: 2 Technical data.

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

⚠	IMPORTANT	**Data loss due to mirroring** The hard disks are automatically formatted during the mirroring process. ● Make sure that no data is lost. ● Always mirror the hard disks before the initial start-up.

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2.   In the tree view, navigate to the node **Storage**.
3.   Select the **General** tab.
4.   Activate the option **Internal Harddisk Mirroring (RAID-1)**.
5.   Click **Apply**.
    ➔ The hard disks will be formatted; this can take about 2 to 4 hours.
    ➔ After the hard disks have been formatted, all recordings will be mirrored.

Hard disk mirroring status
1.   Select the **RAID1** tab.
    ➔ The status of the internal hard disk mirroring will be displayed in the **Internal HD Mirroring** group field (see Fig. 54).

11.5   S.M.A.R.T. status

CX FDV

S.M.A.R.T. stands for Self-Monitoring, Analysis and Reporting Technology.

The continuous monitoring of the hard disks ensures that faults and defects are detected at an early stage. In the event of a fault or defect a message will be sent to the SISTORE CX Client.

Prerequisite:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2.   In the tree view, navigate to the node **Storage**.
3.   To display the S.M.A.R.T. status of the 1st hard disk, select the tab **HDD1**.
4.   To display the S.M.A.R.T. status of the 2nd hard disk, select the tab **HDD2**.
    ➔ The S.M.A.R.T status of the corresponding hard drive will be displayed (see Fig. 53).

	The S.M.A.R.T status **Attention** means that the hard disk is defective and needs to be exchanged (see Section: 11.6 Changing the hard disk).

11.6 Changing the hard disk

	IMPORTANT	**Data loss after a rebuild**
		During a rebuild, individual images may be lost.

Prerequisite:

A hard disk is defective, i.e. the S.M.A.R.T status displayed is **Attention** (see Section: 11.5 S.M.A.R.T. status).

1. Select the **RAID1** tab.

→ The following dialog box opens.

Fig. 54 Storage – Exchange internal hard disk

2. Click on **Set Faulty** under the defective hard disk in the **Hard Disks** group field.

3. Click on **Shutdown Device** in the **Device** group field.

➔ The SISTORE device will shut down.

4. Disconnect the power plug from the SISTORE.

5. Exchange the defective hard disk.

Hard Disk 2 Hard Disk 1	Hard Disk 1 Hard Disk 2
SISTORE CX4	**SISTORE CX8**
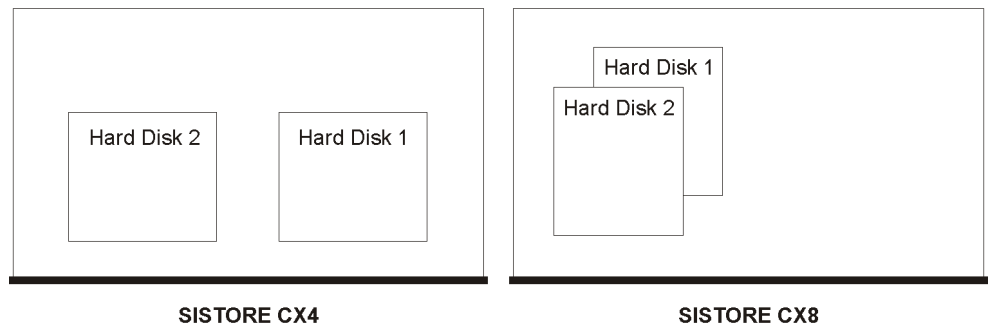
Fig. 55   SISTORE CX4 and SISTORE CX8 hard-disk positions

6. Connect the power plug to the SISTORE device again.

➔ The SISTORE device will be started.

7. Click on **Hot-Add** in the **Hard Disks** group field.

➔ The hard disk will be added while the system is running.

➔ The data will be synchronized.

➔ The status of the synchronization will be displayed in the **Disk Array** group field.

i	During data synchronization the performance of the SISTORE device may get slower (e.g. in Triplex mode).

11.7   Displaying status information on the compact flash card

CX1 FDV

Prerequisites:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the
      software.
2.   In the tree view, navigate to the node **Storage**.
3.   Select the **Compact Flash** tab.
   → The status information of the compact flash card will be displayed.
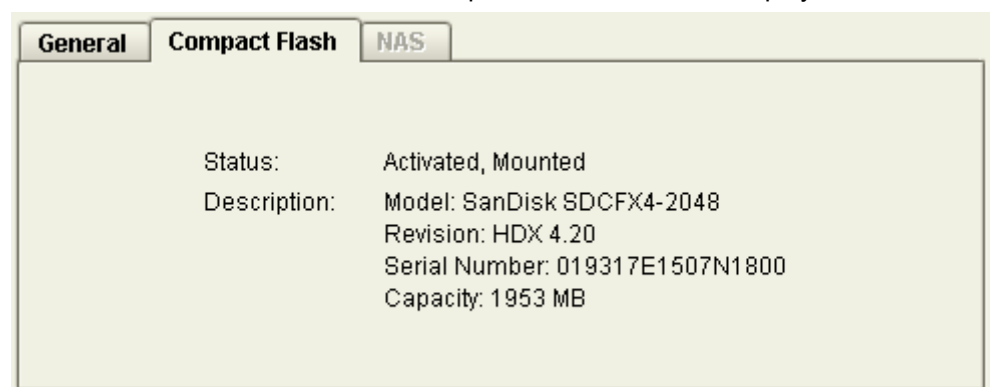
Fig. 56   Storage – Compact Flash status information

11.8   Configuring an external SCSI device

CX8

Prerequisites:

Your SISTORE CX8 has an active SCSI port.

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

> **i**   If the SCSI device has not yet been configured, please refer to the installation manual issued by
> transtec for further information.

1.   Choose a logical drive of 1 TB max.
2.   Format the drive.
3.   Select RAID Level 5 and spare drive as recommended by Siemens.

11.8.1 Displaying status information

CX8

Prerequisites:

Your SISTORE CX8 has an active SCSI port.

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Storage**.
3. Activate the option **External SCSI Storage**.
4. Select the **SCSI** tab.
   ➔ The status information will be displayed in the group field **External SCSI device**.

General	NAS	SCSI

External SCSI device

Status: Activated and mounted
Description: External SCSI Storage

Partitions:

Partition ID	Device	Mount Point	Capacity	Status	Activate
1	/dev/sda1	/data	189 GB	Activated and mounted	✓
2	/dev/sdb1	/data/video2	189 GB	Activated and mounted	✓
3	/dev/sdc1	/data/video3	189 GB	Activated and mounted	✓
4	/dev/sdd1	/data/video4	279 GB	Activated and mounted	✓

Apply

Fig. 57   SCSI device – Status information

11.8.2 Activating and deactivating hard disk partitions

CX8

Prerequisites:

Your SISTORE CX8 has an active SCSI port.

A connection to the SISTORE device has been established (see Section: 4.1 Connecting to SISTORE device).

The data medium **External SCSI device** is activated (see Section: 11.2 Activating a storage medium).

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Storage**.
3. Select the **SCSI** tab.
4. To activate a partition, mark the appropriate checkbox in the column under **Activate** (see Fig. 57).
5. To deactivate a partition, unmark the appropriate checkbox in the column under **Activate** (see Fig. 57).
6. Click **Apply**.
   ➔ The hard disk partitions are now activated or deactivated.

11.9 Configuring Network Attached Storage

CX | FDV

To enable the storage of video data on the Network Attached Storage (NAS), NAS needs to be configured using both the NAS software Windows 2003 Storage Server (see Section: 20.1 Configuring NAS with Windows 2003 Storage Server) and the SISTORE CX configuration software (see Section: 20.2 Configuring NAS using SISTORE CX Config).

12 User administration and administration of rights

CX FDV

The user administration allows individual users to be granted permissions for SISTORE CX. If a user does not have a particular permission, such as the permission to configure rules, then this function is not visible to that user in the SISTORE CX Client.

A distinction is made between local and global user administration. See Section: 12.1 Local user administration and Section: 12.2 Global user administration.

ℹ️ In systems with a large number of SISTORE devices we recommend using global user administration.

If a system is switched from local user administration to global user administration, then the names of all the inputs need to be set up again.

12.1 Local user administration

CX FDV

With local user administration, the users and permissions are configured for each SISTORE device individually.
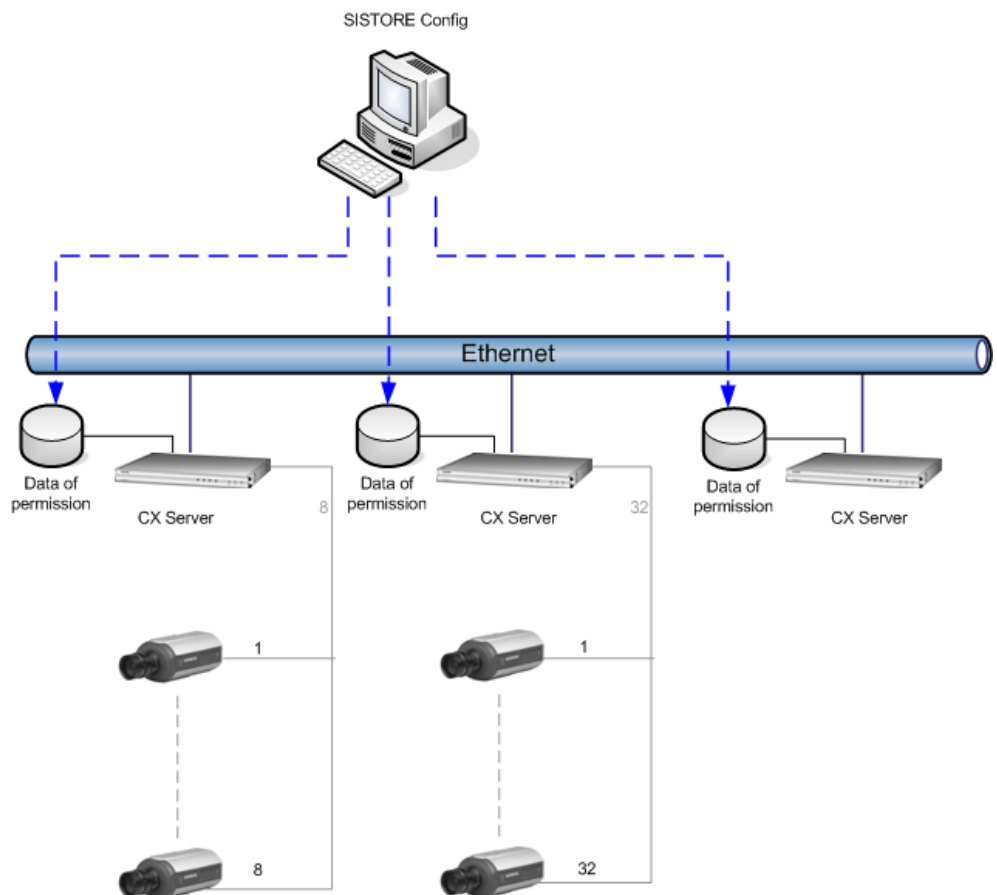
Fig. 58   Local user administration

12.2 Global user administration

CX FDV

With global user administration, the users and permissions are set up for the whole system on the SISTORE SX domain server.

The rights database is managed by the SISTORE domain server, with local copies stored on the individual SISTORE servers. This ensures that user administration is still possible even if there is no connection to the SISTORE domain server.
See Section: 4.7 SISTORE domain server activation.

⚠	**IMPORTANT**	**Recording error due to loss of performance**
		If the SISTORE domain server is installed on a SISTORE device, there may be a significant loss of performance.
		● Install the SISTORE domain server on a separate PC.
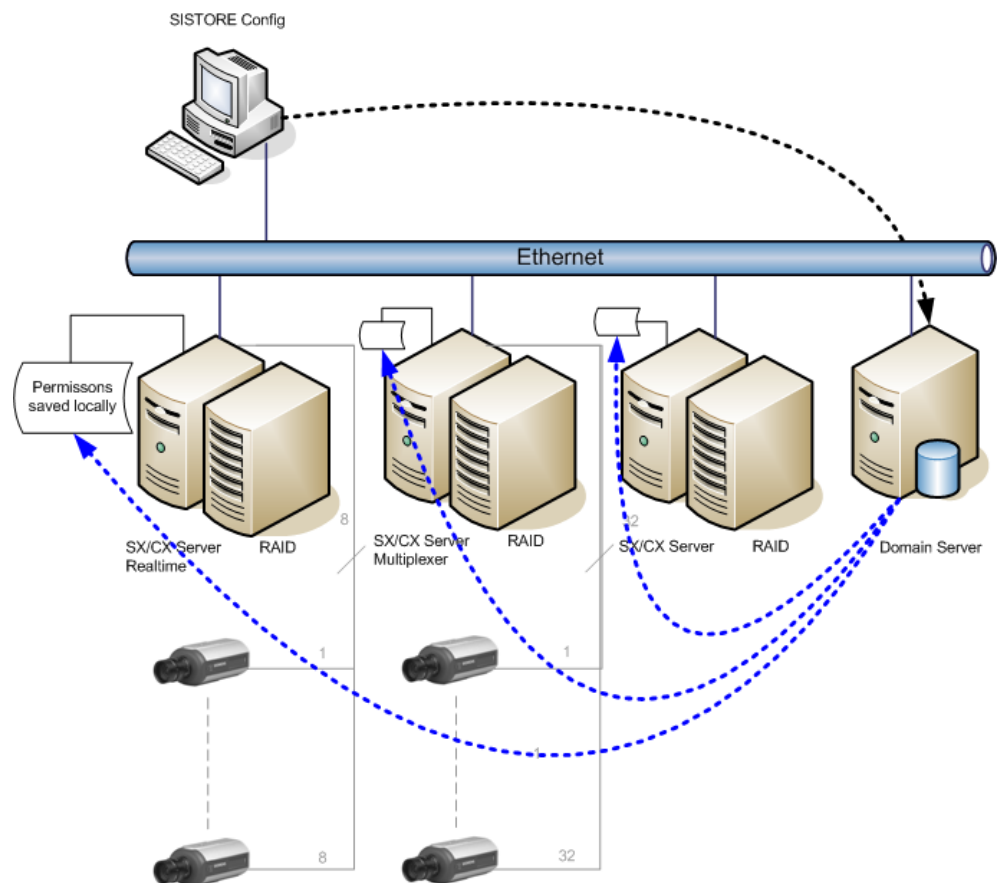
Fig. 59   Global user administration

⚠	**IMPORTANT**	**Logon to SISTORE CX Client not possible**
		Updating a domain server service may take up to 15 minutes, depending on the system configuration. You will not be able to log on to the SISTORE CX Client until the update is completed.

12.3   User administration

12.3.1   Local and global user administration nodes in the tree structure

CX FDV

Local user administration

The node **User administration** in the SISTORE CX Config tree structure is a sub-node of the SISTORE device.
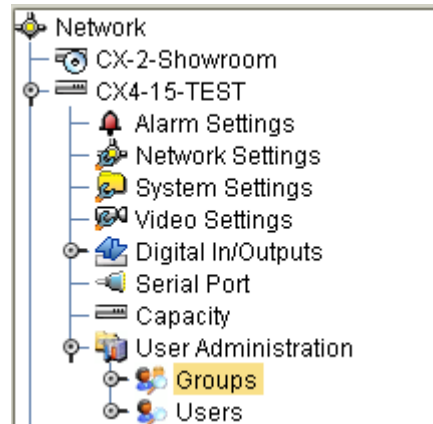
Fig. 60   Tree view – local user administration

Global user administration

The node **User administration** in the SISTORE CX Config tree structure is a sub-node of the **Network** node.
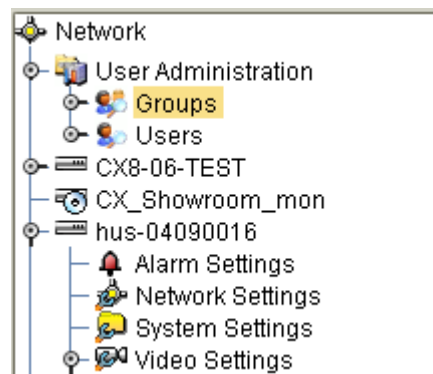
Fig. 61   Tree view – global user administration

107

12.3.2   Adding new user accounts

CX FDV

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.

2. In the tree view, navigate to the node **User administration**.

3. Open the sub-node **Users**.
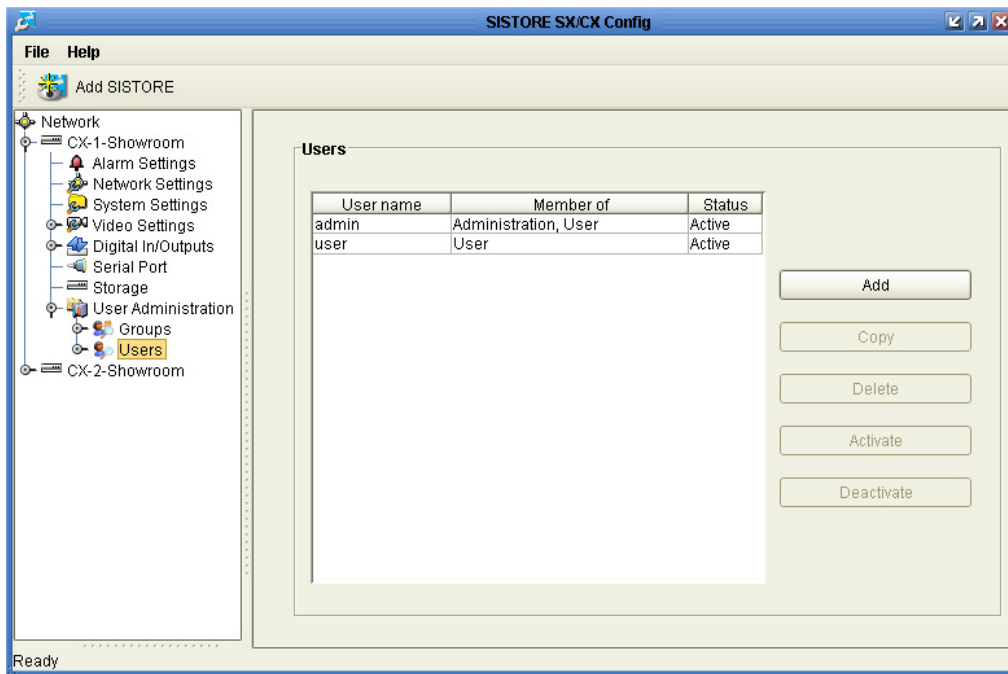
Fig. 62   User administration – Users

4. Click **Add**.

→ The **Add User Account** dialog box opens.

Fig. 63   "Add User Account" dialog box

ℹ
- The entry is case-sensitive.
- Length of the user name: min. 4 characters, max. 64 characters
- Length of the password: min. 4 characters, max. 16 characters. For security reasons, the password will always be displayed with 16 asterisks regardless of its actual length.

---

5.   Enter a user name.

6.   Enter the password twice.

7.   To assign a group to a user account, select one or several user groups in the **Available groups** list.

8.   Click on the button **>>**.

→ The user group will be displayed in the **Assigned groups** list and has been assigned to the user account.

9.   Click on **Create**.

→ The user account will be displayed in the table **Users** and in the tree structure.

12.3.3   Changing user accounts

CX FDV

| i | The user name cannot be changed. |

| i | The administrator can change the passwords of all users. |
| | The user may alter his password using the SISTORE CX Client. Please also refer to the SISTORE CX Client User Manual. |

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **User administration**.
3. Open the sub-node **Users**.
4. Select a user account.
5. Make the desired changes. See Section: 12.3.2 Adding new user accounts.
6. Click **Apply**.

| i | **Global user administration** |
| | The duration of an update of the rights depends on the utilization of the network and the SISTORE system. |

12.3.4   Deleting user accounts

CX FDV

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **User administration**.
3. Open the sub-node **Users**.
4. Select a user account from the table.
5. Click on **Delete**.
6. Answer "Yes" in the confirmation box.
   ➔ The user account will no longer be displayed in the table **Users** and in the tree structure.

12.3.5   Copying user accounts

| CX | FDV |

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **User administration**.
3. Open the sub-node **Users**.
4. Select a user account from the table.
5. Click on **Copy**.
   → The **Copy User Account** dialog box opens.
   → The permissions of the copied user account will be applied.
6. Enter a new user name and password. See Section: 12.3.2 Adding new user accounts.
7. Click **Apply**.
   → The user account will be displayed in the table **Users**.

12.3.6   Deactivating/activating user accounts

| CX | FDV |

Deactivate user accounts
1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **User administration**.
3. Open the sub-node **Users**.
4. Select a user account from the table.
5. Click on **Deactivate**.
   → The status in the table **Users** changes to **Inactive**.

Activate user accounts
1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **User administration**.
3. Open the sub-node **Users**.
4. Select a user account from the table.
5. Click on **Activate**.
   → The status in the table **Users** changes to **Active**.

12.4 Administration of rights

12.4.1 Definition of rights

CX FDV

The following permissions can be assigned to any user or user group:

Permission		Software	Explanation
Recording:	Start recording	SISTORE CX Client	Manually starting a recording **NOTE:** The user must additionally have been granted the permission "Use video input".
	Use replay control		Play recording
	Delete recordings		Delete recording from the hit list
	Lock recording		Write-protect recordings in the hit list
	Edit comment		Edit comment on a recording
	Search for recordings		Use search function
User administration:	Show	SISTORE Config	Show user administration
	Edit		Create and manage users and permissions
Digital outputs:	Change state	SISTORE CX Client	Switch digital outputs
Cameras:	Show configuration		Show camera configuration **NOTE:** The user must additionally have been granted the permission "Use video input".
	Edit configuration		Edit camera configuration
PTZ:	Configure camera presets		Configure camera presets
	Use camera presets		Use camera presets
	Use camera control		Allow camera control
	Use OSD control		Use OSD function
Rules:	Show configuration		Show configuration
	Edit configuration		Edit configuration
	Trigger rules		Trigger rules
Scheduler:	Show configuration		Show scheduler configuration
	Edit configuration		Edit scheduler configuration
SISTORE devices:	Configure	SISTORE Config	Configure SISTORE device
	Storage: Show configuration		Show SISTORE hard disk configuration
Video input:	Use video input	SISTORE CX Client	Display live video
Video output:	Use video output		Display live video on analog monitor

12.4.2   Adding new groups

CX FDV

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the software.

2.   In the tree view, navigate to the node **User administration**.

3.   Open the sub-node **Groups**.
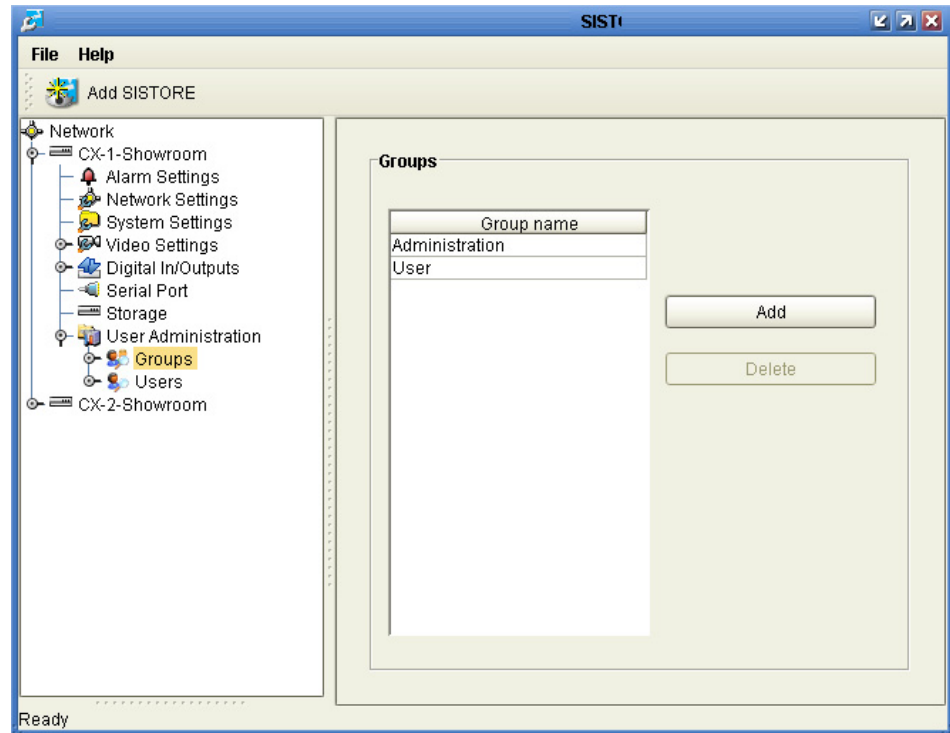
Fig. 64   User administration – Groups

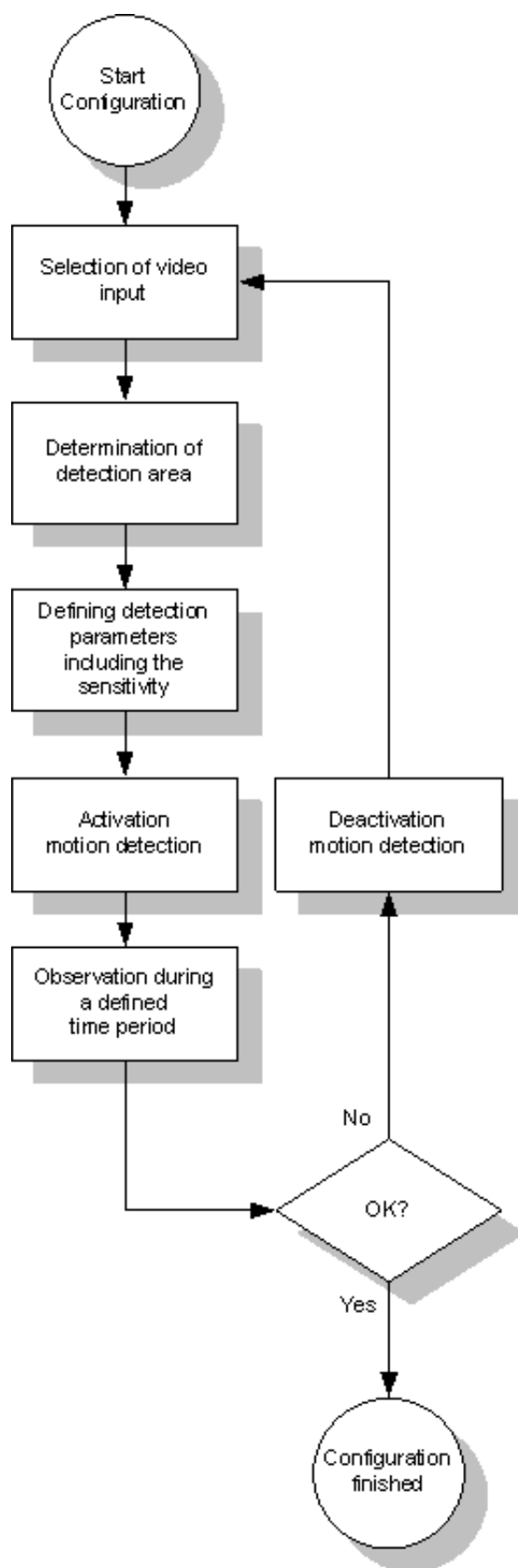4.   Click **Add**.

➔ The **Add Group** dialog box opens.
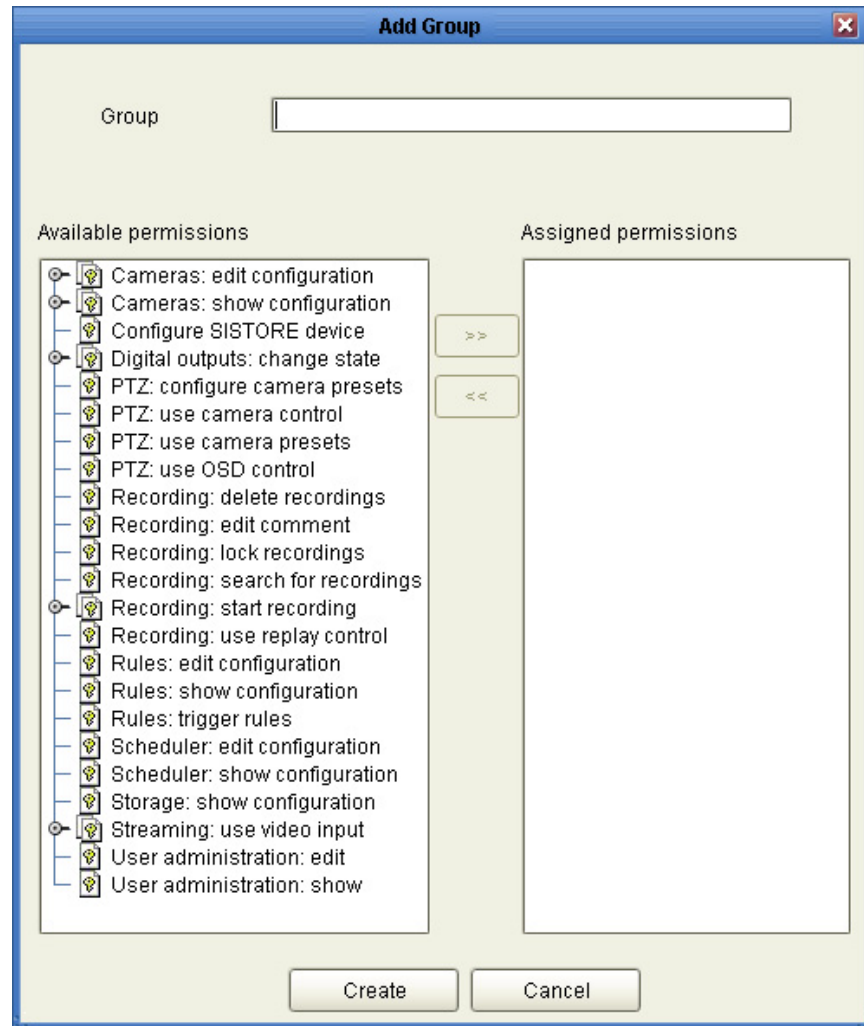
Fig. 65   "Add Group" dialog box

> **ℹ**
>
> The entry is case-sensitive.
> Length of the group name: min. 3 characters, max. 32 characters.

5. Enter a name for the group.

6. To assign permissions to a group, select one or several permissions in the **Available permissions** list.

7. If a group is to be assigned permissions for individual video inputs or digital outputs only, these inputs or outputs must be selected specifically.
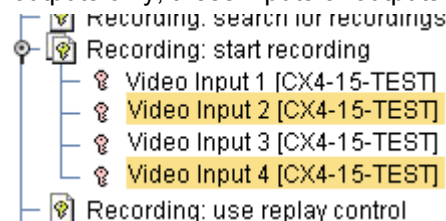
8. Click on the button **>>**.

➔ The permission will be displayed in the **Assigned permissions** list and has been assigned to the group.

9. Click on **Create**.

➔ The group will be displayed in the table **Groups** and in the tree structure.

12.4.3 Assigning group members to user groups

CX FDV

Prerequisite:

A group has been created. See Section: 12.4.2 Adding new groups.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **User administration**.
3. Open the sub-node **Groups**.
4. Select a user group.
5. Select the **Members** tab.
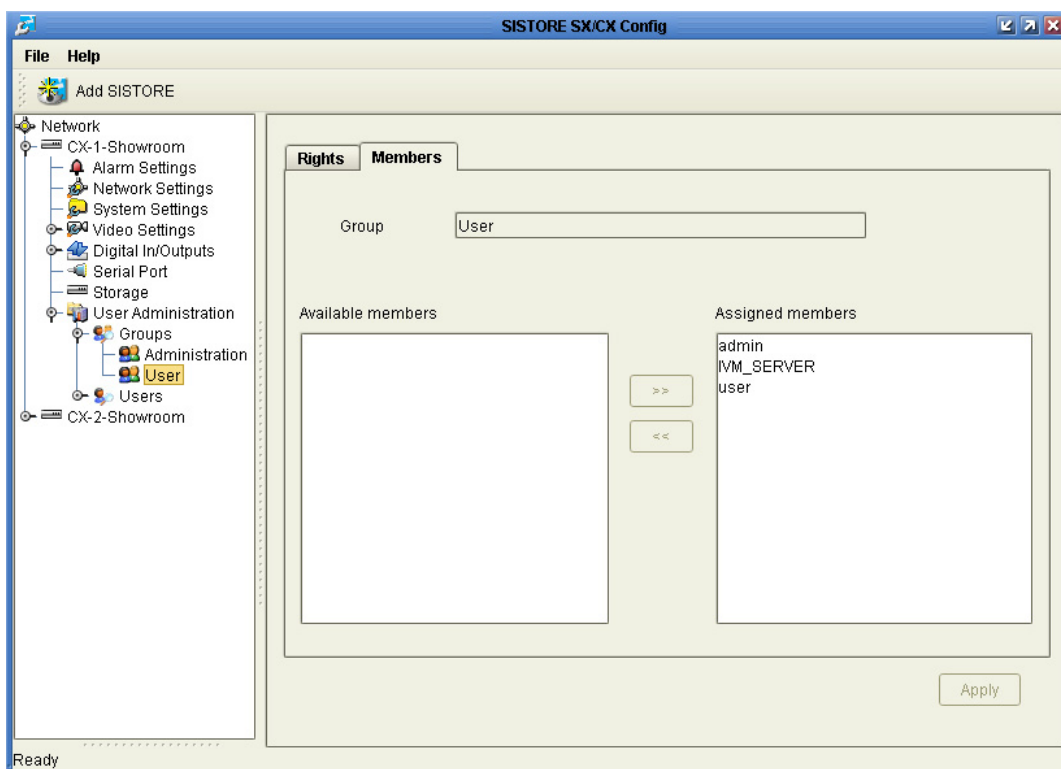
Fig. 66   Groups – "Members" tab

6. To assign members to a group, select one or several members in the **Available members** list.
7. Click on the button **>>**.
   ➔ The member will be displayed in the **Assigned members** list.
8. Click **Apply**.

12.4.4   Changing groups

CX FDV

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **User administration**.
3. Open the sub-node **Groups**.
4. Select a user group.
5. Select the **Rights** tab.
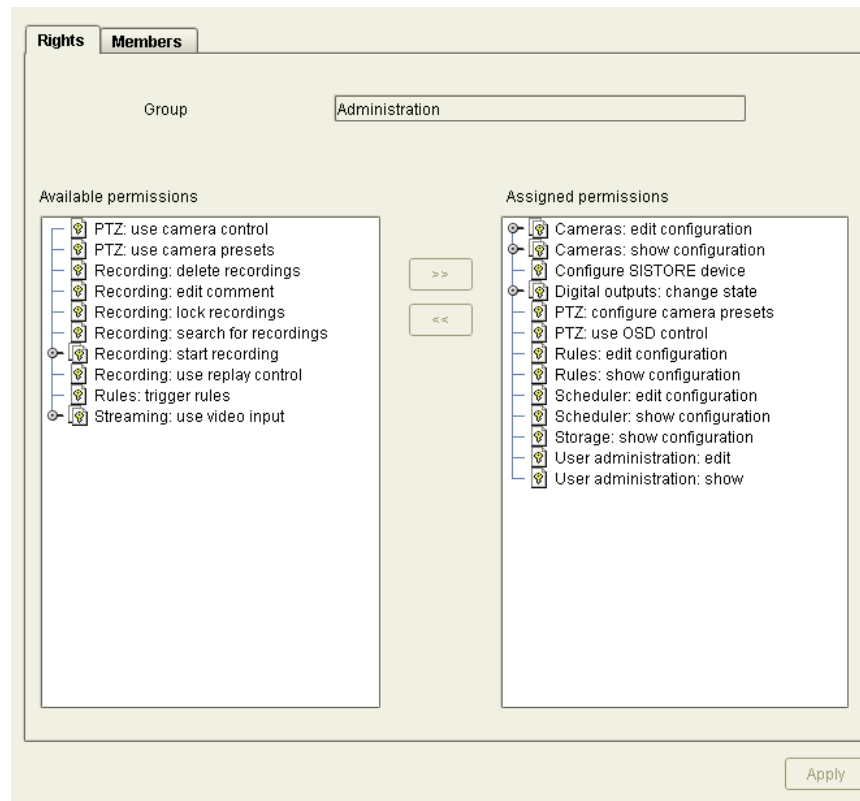
Fig. 67   Groups – "Rights" tab

| i | The name of the group cannot be changed. |

---

6. Reassign the permissions.
7. Select the **Members** tab.
8. Reassign the members. See Section: 12.4.3 Assigning group members to user groups.
9. Click **Apply**.

| i | **Global user administration** |
| | The duration of an update of the rights depends on the utilization of the network and the SISTORE system. |

12.4.5   Deleting groups

CX FDV

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2.   In the tree view, navigate to the node **User administration**.
3.   Open the sub-node **Groups**.
4.   Select a user group from the table.
5.   Click on **Delete**.
6.   Answer "Yes" in the confirmation box.

➔ The group will no longer be displayed in the table **Groups**.

➔ The user group has been deleted.

13 Configuring motion detection

CX FDV

The motion detection function is used to ascertain whether an object has moved within a detection area (specific area in a video image). Depending on the detection parameters set (sensitivity, object size and activation time) this movement may cause an alarm to be triggered.

You can now select motion detection as an event type for rule configuration. See Section: 18 Rule configuration.

Configuration process

```
                    ┌─────────────┐
                    │    Start    │
                    │ Configuration│
                    └──────┬──────┘
                           ▼
                  ┌──────────────────┐◄──────────────┐
                  │ Selection of video│               │
                  │      input        │               │
                  └────────┬─────────┘               │
                           ▼                          │
                  ┌──────────────────┐                │
                  │ Determination of │                │
                  │  detection area  │                │
                  └────────┬─────────┘                │
                           ▼                          │
                  ┌──────────────────┐                │
                  │ Defining detection│               │
                  │    parameters    │                │
                  │  including the   │                │
                  │    sensitivity   │                │
                  └────────┬─────────┘                │
                           ▼                  ┌──────────────────┐
                  ┌──────────────────┐        │   Deactivation   │
                  │    Activation    │        │ motion detection │
                  │ motion detection │        └────────▲─────────┘
                  └────────┬─────────┘                 │
                           ▼                           │
                  ┌──────────────────┐                 │
                  │ Observation during│                │
                  │    a defined     │                │
                  │   time period    │                │
                  └────────┬─────────┘                 │
                           │            No             │
                           │          ┌──────┐         │
                           └─────────►│  OK? │─────────┘
                                      └───┬──┘
                                       Yes│
                                          ▼
                                   ┌─────────────┐
                                   │Configuration│
                                   │  finished   │
                                   └─────────────┘
```

13.1 Colour of the motion detection icon

CX FDV

The symbol for the motion detection in the tree structure provides the following information:

No colour	🏃	Motion detection deactivated
Red	🏃	Motion detection activated, movement detected, alarm triggered
Green	🏃	Motion detection activated, no movement detected, no alarm

13.2 Selecting the detection area

CX FDV

> **i** If no detection area has been defined for the motion detection, the entire live video will be used as detection area.

Prerequisite:

A video input of a SISTORE device which supports the motion detection function has been selected.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Video input**. See Section: 8.3.2 .
3. Click on **Motion Detection**.
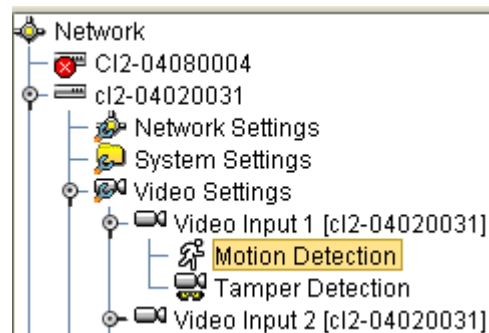
4. Select the **Detection area** tab.
   → The live video of the camera for which you want to determine a detection area is now displayed.
5. Add a new detection area using the icons on the right of the live video.
6. Using these icons, you can freely configure the detection area and position it anywhere in the live video. You can add and insert further points and move existing points within the detection area.
7. Click **Apply**.

> **i** You can stipulate several detection areas per video input (live video). See the figure below.
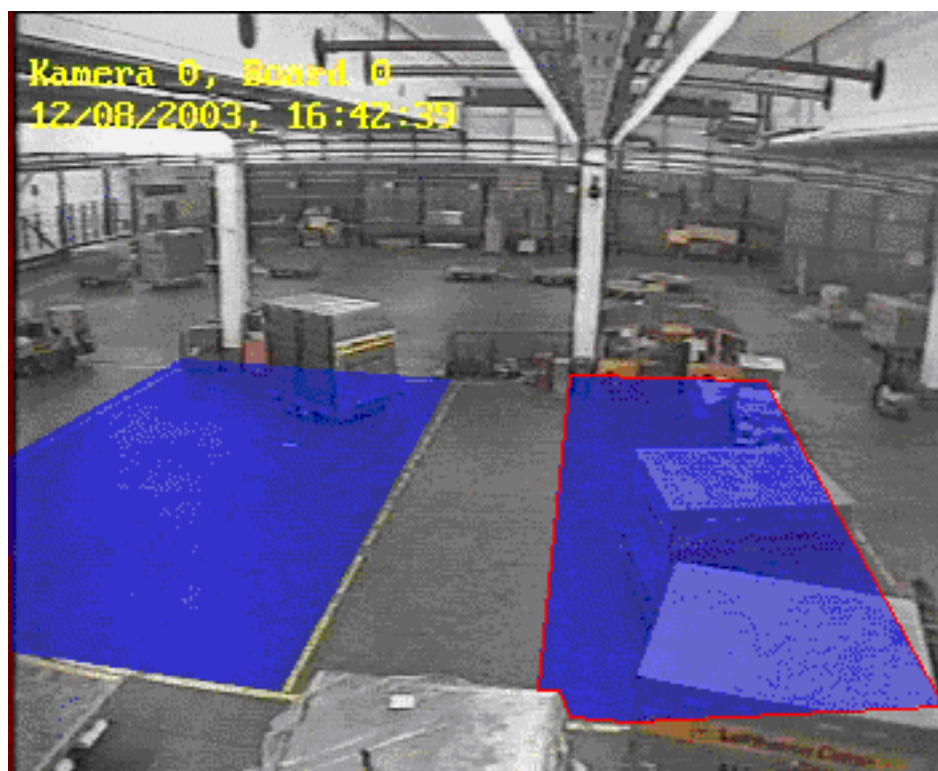
Fig. 68   Two detection areas

13.3   Defining the detection parameters

CX FDV

ℹ️ When you switch to configuration mode, motion detection is automatically activated. First deactivate all associated rules in the SISTORE CX Client so that no recordings are accidentally triggered. It is not possible to suppress the alerts sent to the video management system IVM.

Prerequisite:

At least one detection area has been defined. See Section: 13.2 Selecting the detection area .

1.   Select the detection areas of the live video for which you want to set the detection parameters. If you have determined several detection areas in one image, then the same parameters will apply to all these areas.

2.   Set the following parameters in the **Detection parameters** tab:
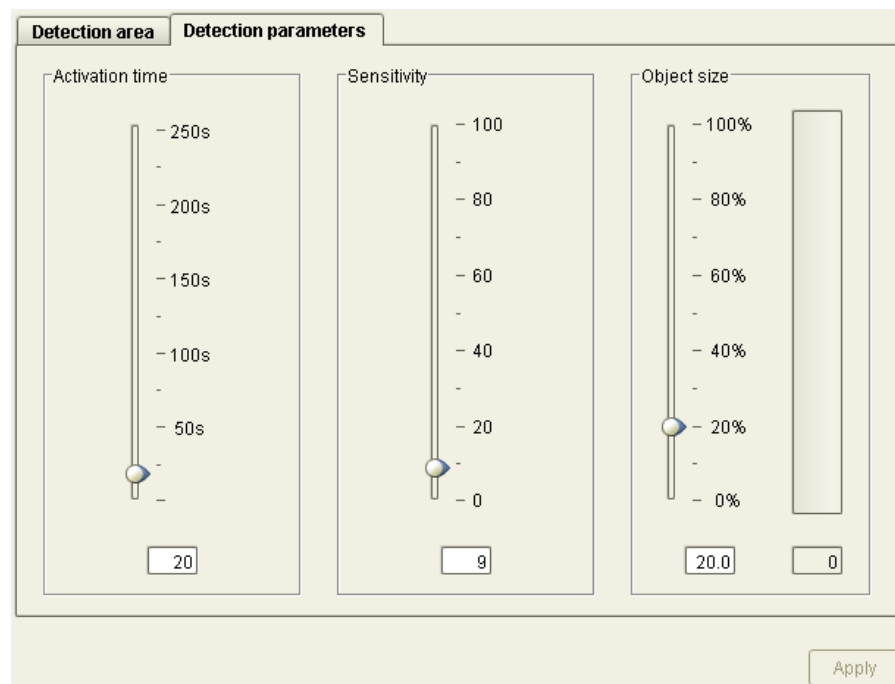
Fig. 69   "Detection parameters" tab

Activation time	Period of time during which an alarm is maintained if no further movement is detected.
	The frame around the detection area remains red during the entire activation time even if there are no moving objects in the image. After this time it automatically changes to green.
Sensitivity	The sensitivity percentage determines the sensitivity threshold for the motion alarm. When this threshold is exceeded an alarm will be triggered. You can observe the effect live in the video.
	A good starting value is 9. This value can be increased for very noisy images.
	Set the control to the lowest setting at which the image noise no longer triggers the motion detection but movement is still reliably detected under all occurring lighting conditions.
Object size	The minimum percentage of the detection area in which motion must be detected to trigger an alarm. Small objects or individual image points with motion can often be considered noise.

3.   Click **Apply**.

13.4   Activating / deactivating motion detection

CX FDV

Prerequisites:

At least one detection area has been defined. See Section: 13.2 Selecting the detection area .

The detection parameters for the detection areas have been defined. See Section: 13.3 Defining the detection parameters .

Activating motion detection

1.   Tick the checkbox **Activate** in the Detection area tab.
2.   Click **Apply**.
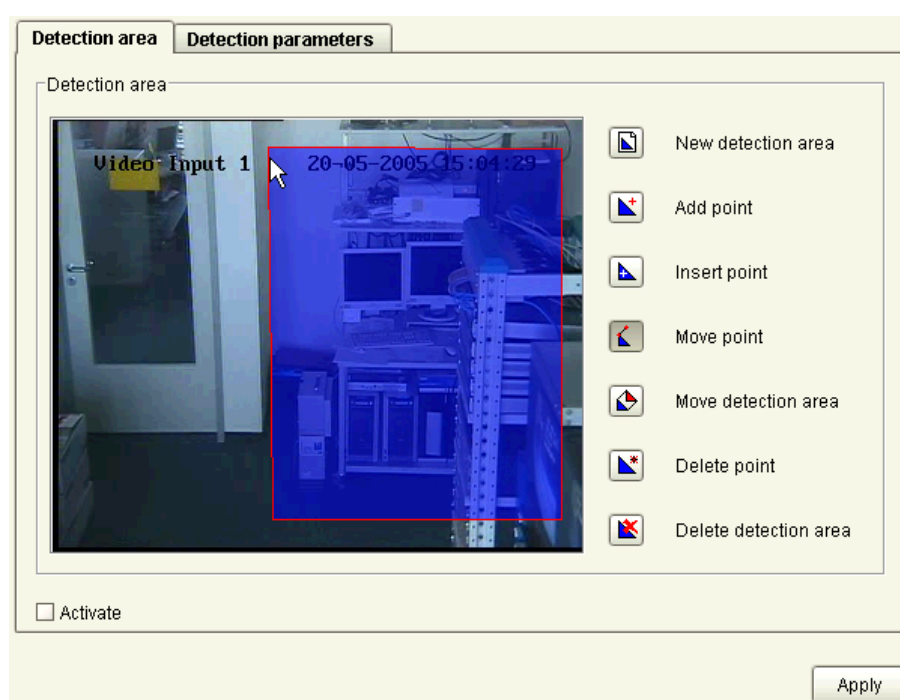
→ The detection area is now active and the detection parameters you have defined will be applied. Movement in this detection area may cause an alarm to be triggered.

→ You can now select motion detection as an event type (MotionDetected/MotionGone) for rule configuration. See Section: 18 Rule configuration.

Deactivating motion detection

1.   To deactivate the motion detection, untick the checkbox **Activate** in the **Detection area** tab.
2.   Click **Apply**.

13.5 Pre-event recording and post-event recording for motion alarms

| CX | FDV |

Pre-event recording and post-event recording are designations for recordings made within a predefined period of time prior to an event and after an event occurs, respectively. In the case of motion detection, this is always the event "Motion Detected".
If the post-event recording time is set too short, the recording may be cut off without the detected motion being recorded completely (1).

If the post-event recording is sufficiently long, the recording will be terminated by stop event. This stop event is defined in a rule.
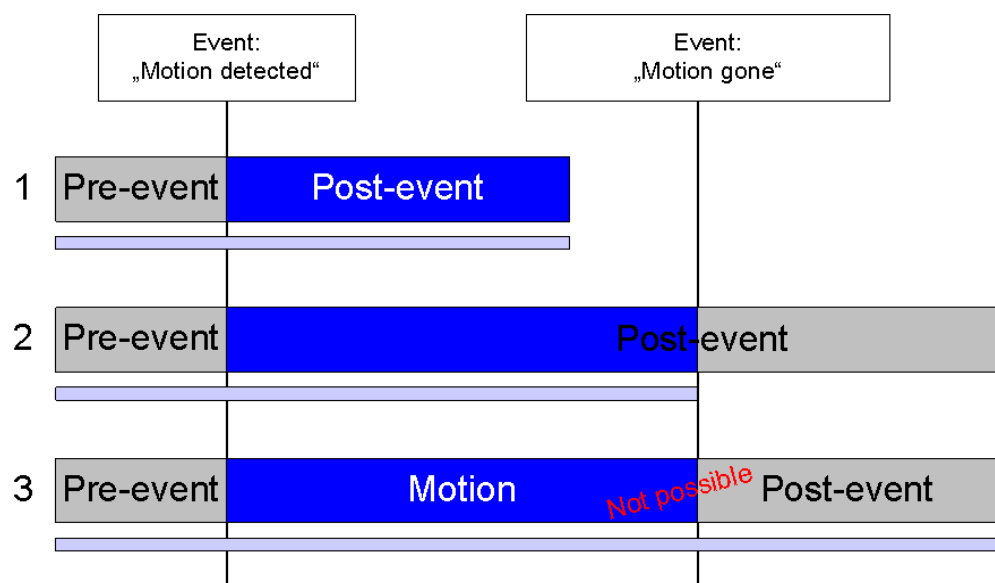
Fig. 70   Possible post-event recording configurations

The graphic shows the possible post event recording configurations.

1   Post-event recording set too short

2   Post-event recording set correctly

3   This variant is not possible.

If no pre-event recording is desired, you can eliminate it. However, depending on system load, it is possible for up to 20 seconds to pass between the time when a motion is detected and recording is started. This aspect must be considered when configuring the rules.

In order to have the complete history on disk, the pre event recording must therefore be at least 36 seconds. In practice, we recommend 1-2 minutes.

| **i** | Never set a pre-event recording of less than 1 minute. |

14 Configuring Enhanced Motion Detection

CX

The Enhanced Motion Detection allows objects moving in the camera picture to be detected and pursued. The pursuing function can be used to trigger alarms. A maximum of 16 objects can be pursued simultaneously.
The licence for the Enhanced Motion Detection will disable the motion detection function currently configured for your SISTORE device(s).

⚠	IMPORTANT	**Deterioration of detection performance in indoor applications**
		When using the Enhanced Motion Detection in indoor applications, the detection performance may deteriorate.
		● The Enhanced Motion Detection should only be used for outdoor applications.

Configuration process

```
                    ┌───────────────┐
                    │     Start     │
                    │ configuration │
                    └───────┬───────┘
                            │
                            ▼
        ┌─────────────────────────────┐
        │      Select video input     │◄───────────┐
        └─────────────┬───────────────┘            │
                      │                             │
                      ▼                             │
        ┌─────────────────────────────┐            │
        │        Define alarm         │            │
        │          program            │            │
        └─────────────┬───────────────┘            │
                      │                             │
                      ▼                             │
        ┌─────────────────────────────┐            │
        │    Define global  alarm     │            │
        │      program settings       │            │
        └─────────────┬───────────────┘            │
                      │                             │
                      ▼                             │
        ┌─────────────────────────────┐            │
        │      Define program-        │            │
        │       specific alarm        │            │
        │      program settings       │            │
        └─────────────┬───────────────┘            │
                      │                             │
                      ▼                             │
        ┌───────────────────┐   ┌───────────────────┐
        │   Enable alarm    │   │   Disable alarm   │
        │     program       │   │     program       │
        └─────────┬─────────┘   └─────────▲─────────┘
                  │                       │
                  ▼                       │
        ┌───────────────────┐             │
        │  Observation for a │            │
        │ defined period of time │        │
        └─────────┬─────────┘             │
                  │              No       │
                  │          ┌─────────┐  │
                  └─────────►│Everything│─┘
                             │   OK?   │
                             └────┬────┘
                                  │ Yes
                                  ▼
                           ┌──────────────┐
                           │Configuration │
                           │  completed   │
                           └──────────────┘
```
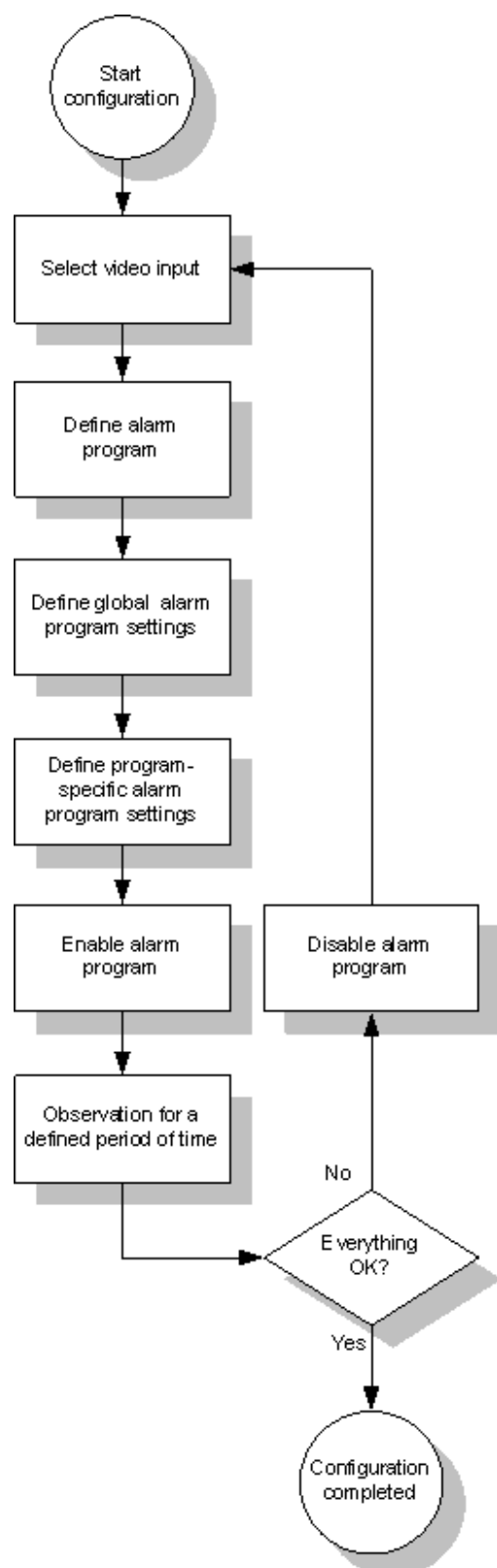
14.1 Colour of the symbol for Enhanced Motion Detection

CX

The symbol for the Enhanced Motion Detection in the tree structure provides the following information:

No colour		Enhanced Motion Detection disabled
Red		Enhanced Motion Detection enabled, movement detected, alarm triggered
Green		Enhanced Motion Detection enabled, no movement detected, no alarm triggered

14.2 Licence key entry

CX

1.   In the tree view, navigate to the node **Video input**.

2.   Click the **License key** button.

3.   The **Input license** dialog box opens.

4.   Enter the licence key using hyphens.

5.   Click **OK**.

→ The Enhanced Motion Detection has now been enabled and is ready for use.

14.3 Starting the Enhanced Motion Detection

CX

Prerequisites:

The licence key has been entered.

An EDS operation mode has been selected. See Section: 8.1 Set operating mode.

> **i**
>
> There are three possible EDS operation modes:
> - The operation mode **EDS Standard Performance Tracking and Encoder** can be activated for **2** and for **4** channels. The detection performance is identical in both cases. When 2 channels are activated the input signal is displayed on the analog output with a detection frame around it.
> - In the **EDS Enhanced Performance Tracking and Encoder** operation mode, the detection performance is improved, this being of advantage in particular in pictures with low contrast and fast-moving objects.
>
> See Section: 3.1 Operating modes and performance characteristics.

A video input of a SISTORE device which supports the motion detection function has been selected.

1.   Start the SISTORE CX Config application. See Section: 3.15 Starting the software.

2.   In the tree view, navigate to the node **Video input**.
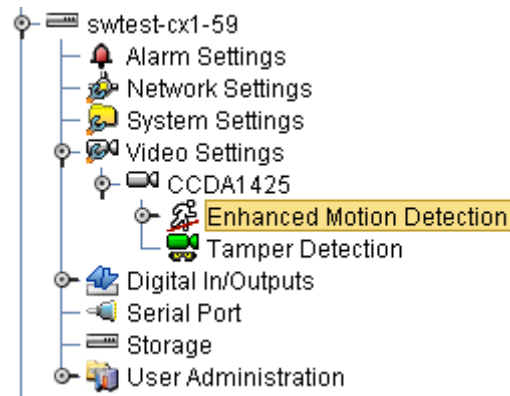
Fig. 71   Enhanced Motion Detection

3. Select **Enhanced Motion Detection**.

    → The tabs **Alarm programs**, **Global Detection Parameters** and **Alarm Handling** will be displayed (see Fig. 72).

14.4   Defining alarm programs

CX

An alarm program is a combination of detection parameters for a particular application.

It may be necessary to define different alarm programs for detecting objects during the day and at night.

> [i]   Up to four alarm programs can be defined for each video input.

Adding alarm programs

1. Select **Enhanced Motion Detection** in the tree structure. See Section: 14.3 Starting the Enhanced Motion Detection.
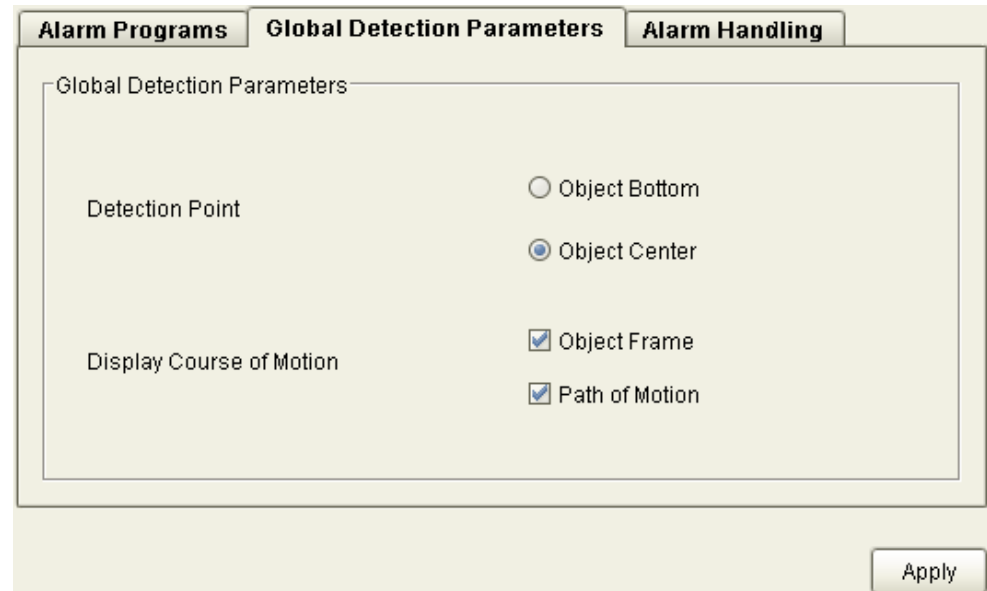
2. Select the **Alarm programs** tab.

Fig. 72   Alarm program settings – "Alarm Programs" tab

3. Click **Add**.

➔ The **Add Program** dialog box opens.

Fig. 73   Alarm program settings – "Add Program" dialog box

4. Add a comment on the alarm program in the **Comment** box.

5. To copy an alarm program, select a template from the **Template** list box.

6. Click **OK**.

➔ A new alarm program has now been defined.

7. Click **Apply**.

➔ The alarm program will now be listed under **Add/Remove Alarm Program**.

➔ The alarm program will appear in the device tree under **Enhanced Motion Detection**.

Fig. 74   Alarm program settings – Alarm Program

8. You can now set the alarm program parameters. See Section: 14.6 Global alarm program settings and Section: 14.7 Program-specific alarm program settings.

Removing alarm programs

1.   Select **Enhanced Motion Detection** in the tree structure. See
     Section: 14.3 Starting the Enhanced Motion Detection.
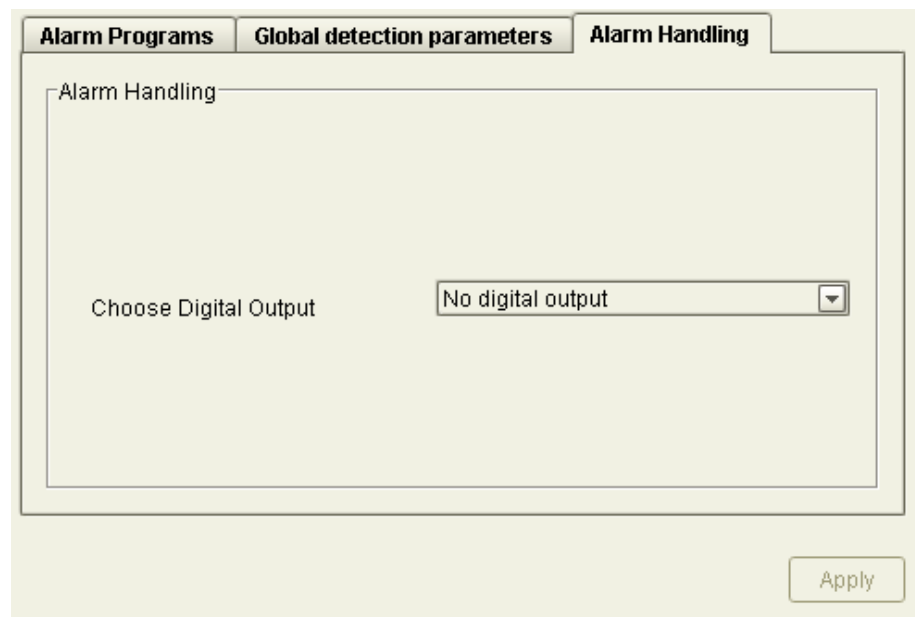2.   Select the **Alarm programs** tab.
3.   Select an alarm program from the list.
4.   Click on **Remove**.
     → The alarm program is now removed.
5.   Click **Apply**.
     → The alarm program will now be listed under **Add/Remove Alarm Program**.
     → The alarm program will appear in the device tree under **Enhanced Motion Detection**.

14.5   Activating an alarm program

CX

Prerequisite:

A least one trip wire or direction field has been defined. See
Section: 14.7.4 Defining trip wires or 14.7.8 Defining the direction field.

There are several possibilities to activate an alarm program:

● Global alarm program settings

     – OR –

● Program-specific alarm program settings

Global alarm program settings

1.   Select **Enhanced Motion Detection** in the tree structure. See
     Section: 14.3 Starting the Enhanced Motion Detection.
2.   Select the **Alarm programs** tab.
3.   Select an alarm program from the list.
4.   Click on the "eye" under **Active**.
     → The selected alarm program is now active. Alarms will be triggered as
     configured in the alarm program settings. See Section: 14.6 Global alarm
     program settings and Section: 14.7 Program-specific alarm program settings.

Program-specific alarm program settings

1.   Select **Enhanced Motion Detection** in the tree structure. See
     Section: 14.3 Starting the Enhanced Motion Detection.
2.   Select an alarm program. See Section: 14.4 Defining alarm programs.
3.   Make the desired program-specific settings.
4.   Click on **Activate**.
     → The alarm program settings will be applied.
     → The selected alarm program is now active. Alarms will be triggered as
     configured in the alarm program settings. See Section: 14.6 Global alarm
     program settings and Section: 14.7 Program-specific alarm program settings.

14.6 Global alarm program settings

14.6.1 Definition of global detection parameters

CX

Global detection parameters

Global detection parameters are settings in the configuration software SISTORE CX Config for the detection of objects that are valid for all alarm programs.

Global detection parameters of the Enhanced Motion Detection are: the detection point and the course of motion.

Detection point

The detection point is a point on or within the object frame that is relevant to the detection.

Detection points are the object centre and the object bottom.

An alarm is triggered once the object centre or the object bottom has entirely crossed the alarm area and passed the trip wire.

Object bottom	Object centre
The object bottom is the centre of the bottom line of the object frame.	The object centre is the centre of the object frame.

Course of motion

The course of motion is the graphical display of the object's motion within the live video.

The course of motion is displayed as a path of motion and/or an object frame.

Path of motion	Object frame
The path of motion is the display of the object's motion in the live video as a line.	The object frame is the rectangular demarcation of an object within the live video.

Meaning of the colour of path of motion and object frame

White	The object is not compliant with the detection parameters set. See Section: 14.7.10 Definition of program-specific detection parameters .
Green	The object is compliant with the detection parameters set and can trigger an alarm. See Section: 14.7.10 Definition of program-specific detection parameters .
Blue	The object is compliant with the detection parameters set and is in the alarm or direction area. An alarm has not been triggered yet. See Sections: 14.7.10 Definition of program-specific detection parameters , 14.7.5 Defining alarm areas and 14.7.7 Defining the direction area.
Red	The object is compliant with the detection parameters set and the alarm criteria (e.g. trip wire crossed). An alarm was triggered. See Sections: 14.7.4 Defining trip wires, 14.7.5 Defining alarm areas and 14.7.7 Defining the direction area.

Example of global detection parameters
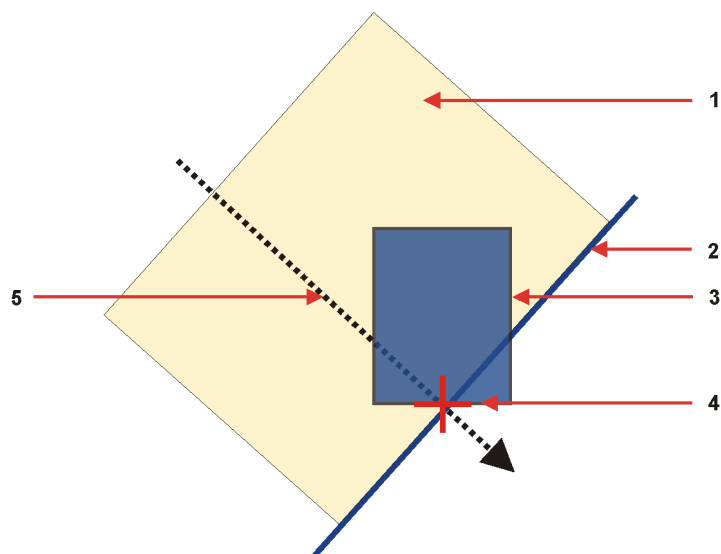
Fig. 75   Detection point and course of motion

1	Alarm area	See Section: 14.7.5 Defining alarm areas.
2	Trip wire	See Section: 14.7.4 Defining trip wires.
3	Object frame	See Section: 14.7.3 Matching the size of the object frame to the perspective mode.
4	Detection point	
5	Path of motion	

Example   **Explanation**
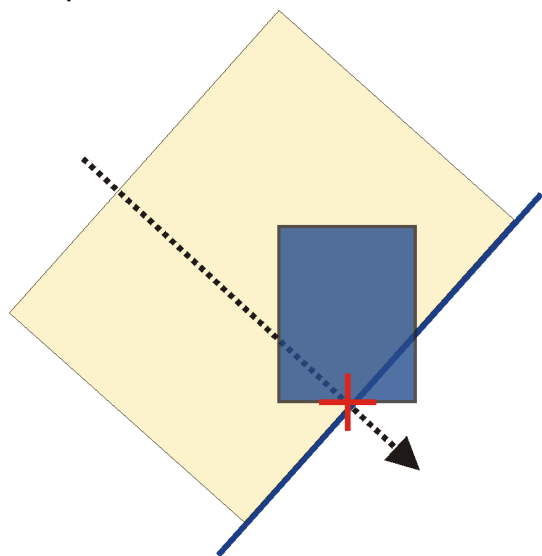
The object bottom has crossed the alarm area.
➔ An alarm is triggered.

Example
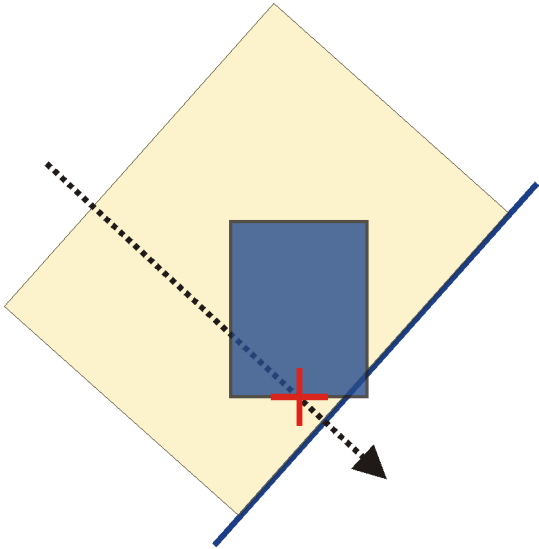
Explanation

The object bottom has not yet crossed the alarm area.
➔ An alarm will **not be triggered yet**.
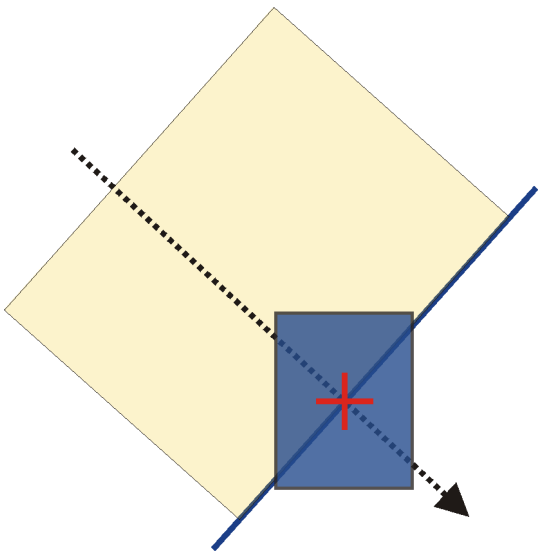
The object centre has crossed the alarm area.
➔ An alarm is triggered.
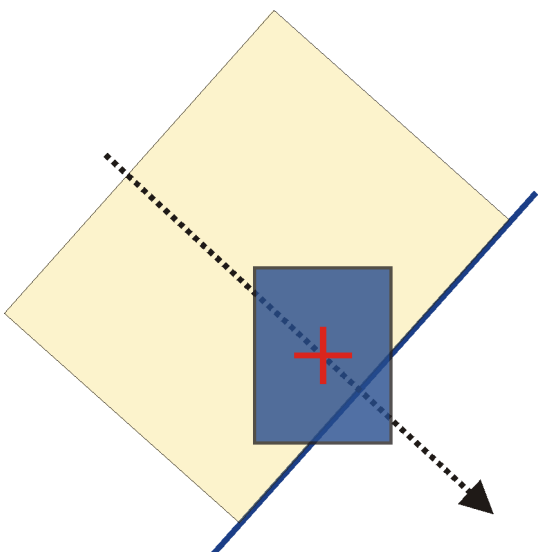
The object centre has not yet crossed the alarm area.
➔ An alarm will **not be triggered yet**.

Definition of global detection parameters

Prerequisite:

An alarm program has been defined. See Section: 14.4 Defining alarm programs.

1. Select **Enhanced Motion Detection** in the tree structure. See
      Section: 14.3 Starting the Enhanced Motion Detection.

2. Select the **Global Detection Parameters** tab.

Fig. 76   Alarm program settings – "Global Detection Parameters" tab

3. Activate either **Object Bottom** or **Object Center**.

4. Tick the checkbox(es) **Object Frame** and/or **Path of Motion**.

5. Click **Apply**.

14.6.2 Definition of the alarm handling

CX

Alarm handling

Alarm handling is a software setting/mode which handles alarm transmission.

Digital output

A digital output is an output on a device where signal transmitters can be connected.

External signal transmitters, such as audible alarms, lamps, door sensors or light barriers, can receive a signal from the device via a relay.

Definition of the alarm handling

Prerequisite:

An alarm program has been defined. See Section: 14.4 Defining alarm programs.

1.   Select **Enhanced Motion Detection** in the tree structure. See Section: 14.3 Starting the Enhanced Motion Detection.
2.   Select the **Alarm Handling** tab.

Fig. 77   Alarm program settings – "Alarm Handling" tab

3.   Select a digital output from the drop-down list.
4.   Click **Apply**.

14.7 Program-specific alarm program settings

CX

Program-specific settings are made individually for each alarm program.

Program-specific settings are:

- Perspective area (see Section: 14.7.1 Definition of perspective areas)
- Perspective modes (see Section: 14.7.2 Defining the perspective mode)
- Trip wire (see Section: 14.7.4 Defining trip wires)
- Alarm area (see Section: 14.7.5 Defining alarm areas)
- Direction area (see Section: 14.7.7 Defining the direction area)
- Direction field (see Section: 14.7.8 Defining the direction field)
- Program-specific detection parameters (see Section: 14.7.10 Definition of program-specific detection parameters)

14.7.1 Definition of perspective areas

CX

Perspective area

The perspective area is an area within the live video where the formation and/or motion of objects is detected and/or tracked.

The user defines two object sizes within the perspective area: one in the foreground and one in the background. In doing so, the size differences in the live video that result from the perspective are analysed correctly.

i Up to four perspective areas can be defined for each live video.

Definition of perspective areas

Prerequisite:

An alarm program has been defined. See Section: 14.4 Defining alarm programs.

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2. Select the **Perspective Areas** tab.

Fig. 78   Alarm program – "Perspective Areas" tab

3.   Click **Add**.

4.   Select a perspective area from the list.

5.   Use the toolbar to draw or change a perspective area.

6.   Click **Apply**.

Removing perspective areas

1.   Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.

2.   Select the **Perspective Areas** tab.

3.   Select a perspective area from the list.

4.   Click on **Remove**.

➔ The perspective area no longer appears in the list.

5.   Click **Apply**.

Show/hide perspective areas

This function provides more clarity when creating or changing perspective areas.

1.   Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.

2.   Select the **Perspective Areas** tab.

3.   Select a perspective area from the list.

4.   Click on the "eye" to show or hide the perspective area.

➔ The perspective area now either disappears or is displayed.

14.7.2   Defining the perspective mode

CX

Perspective mode

Perspective modes are landscape perspective and façade perspective.

In the perspective mode it can be determined in which perspective an object has to appear within a predefined perspective area to be detected. The decisive factor is the distance between object and camera.

Landscape perspective	Façade perspective
The landscape perspective is a perspective mode.	The façade perspective is a perspective mode.
With the landscape perspective the object size is evaluated in a predefined perspective area of the live video. The object size in the live video depends on the object's distance to the camera. With the landscape perspective the object size in the live video changes noticeably.	With the landscape perspective the object size is evaluated in a predefined perspective area of the live video. The object size in the live video depends on the object's distance to the camera. With the façade perspective the object size in the live video rarely changes.
➔ Two object frames of different sizes appear in the perspective area. Both object frames have the same aspect ratio.	➔ Two object frames of the same size appear in the perspective area.

Defining the perspective mode

Prerequisites:

An alarm program has been defined. See Section: 14.4 Defining alarm programs.

A perspective area has been defined. See Section: 14.7.1 Definition of perspective areas.

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2. Select the **Perspective Modes** tab.

Fig. 79   Alarm program – "Perspective Modes" tab

3. Select the **perspective area** for which you want to define a perspective mode.
4. Activate either **Landscape Perspective** or **Façade Perspective**.
5. Click **Apply**.
6. Match the size of the object frame to the perspective mode. See
   Section: 14.7.3 Matching the size of the object frame to the perspective mode.

14.7.3   Matching the size of the object frame to the perspective mode

CX

Object frame

The object frame is the rectangular demarcation of an object within the live video.

The course of motion is displayed as a path of motion and/or an object frame.

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2. Select the **Perspective Modes** tab.
3. Place an object in the monitored area.
4. You can enlarge or reduce the size of the image by clicking **Zoom In** and **Zoom Out**, respectively.
5. Use the toolbar icons to match the size of the object frames in the live video to the actual object size.

i   The width-to-height ratio of the light-coloured object frame is automatically matched to the dark-coloured object frame and can therefore not be changed.

6. Click **Apply**.
7. Determine the minimum size of an object to be detected. See Section: 14.7.10 Definition of program-specific detection parameters .

14.7.4   Defining trip wires

CX

Trip wire

The trip wire is a line within the alarm area. An alarm is triggered only if the object bottom or centre has entirely crossed the predefined alarm area and the predefined trip wire.

i   Up to eight trip wires can be defined.

Defining trip wires

Prerequisites:

An alarm program has been defined. See Section: 14.4 Defining alarm programs.

A perspective area has been defined. See Section: 14.7.1 Definition of perspective areas.

A perspective mode has been defined. See Section: 14.7.2 Defining the perspective mode.

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2. Select the **Trip Wire** tab.
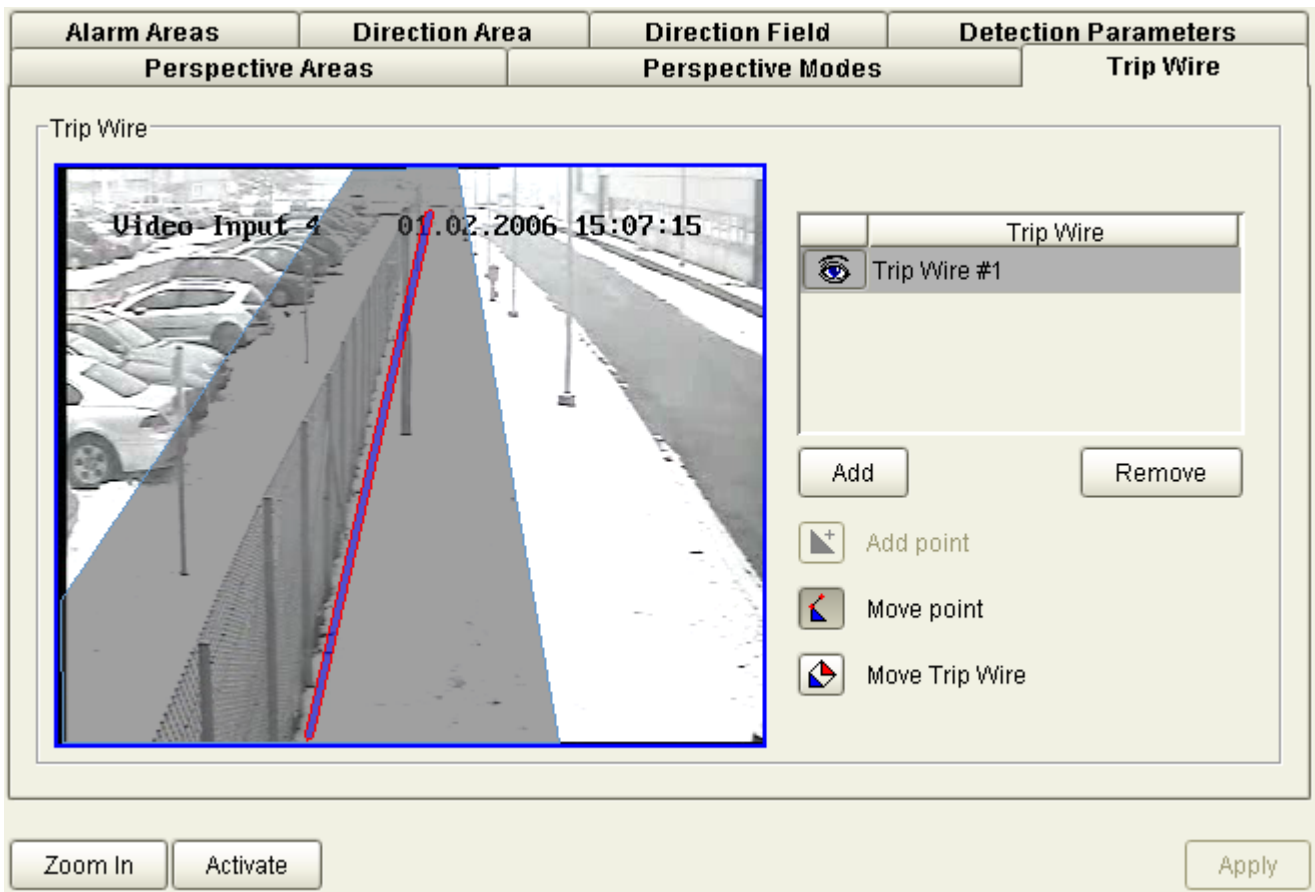
Fig. 80   Alarm program – "Trip Wire" tab

3.   Click **Add**.

4.   Select a trip wire from the list.

5.   You can enlarge or reduce the size of the image by clicking **Zoom In** and **Zoom Out**, respectively.

6.   Use the toolbar icons to draw/change the trip wire(s).

7.   Click **Apply**.

Removing the trip wire

1.   Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.

2.   Select the **Trip Wire** tab.

3.   Select a trip wire from the list.

4.   Click on **Remove**.

5.   Click **Apply**.

Show/hide trip wire

1.   Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.

2.   Select the **Trip Wire** tab.

3.   Select a trip wire from the list.

4.   Click on the "eye" to show or hide the trip wire.

➔ The trip wire now either disappears or is displayed.

Change ID of trip wire

1.   Double-click on a trip wire in the list.

   ➜ The **Input** dialog will open.

2.   Enter a new ID in the input field.

3.   Click **OK**.

14.7.5   Defining alarm areas

CX

Alarm area

The alarm area is a defined area in the live video between the origin of the arrow and the trip wire.

An alarm is triggered only if the object bottom or centre has entirely crossed the predefined alarm area and the predefined trip wire. See Section: 14.6.1 Definition of global detection parameters.
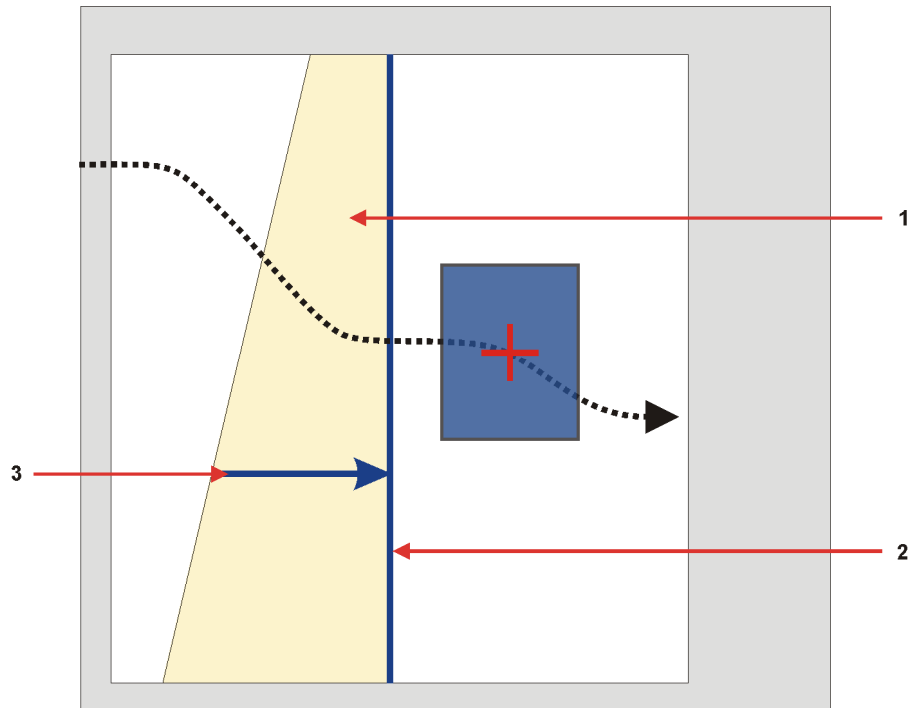
Fig. 81   Alarm area – Landscape perspective

1	Alarm area	See Section: 14.7.5 Defining alarm areas.
2	Trip wire	See Section: 14.7.4 Defining trip wires.
3	Arrow	See Section: 14.7.5 Defining alarm areas.

Defining alarm areas

Prerequisites:

An alarm program has been defined. See Section: 14.4 Defining alarm programs.

A perspective area has been defined. See Section: 14.7.1 Definition of perspective areas.

A perspective mode has been defined. See Section: 14.7.2 Defining the perspective mode.

A trip wire has been defined. See Section: 14.7.4 Defining trip wires.

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2. Select the **Alarm Areas** tab.
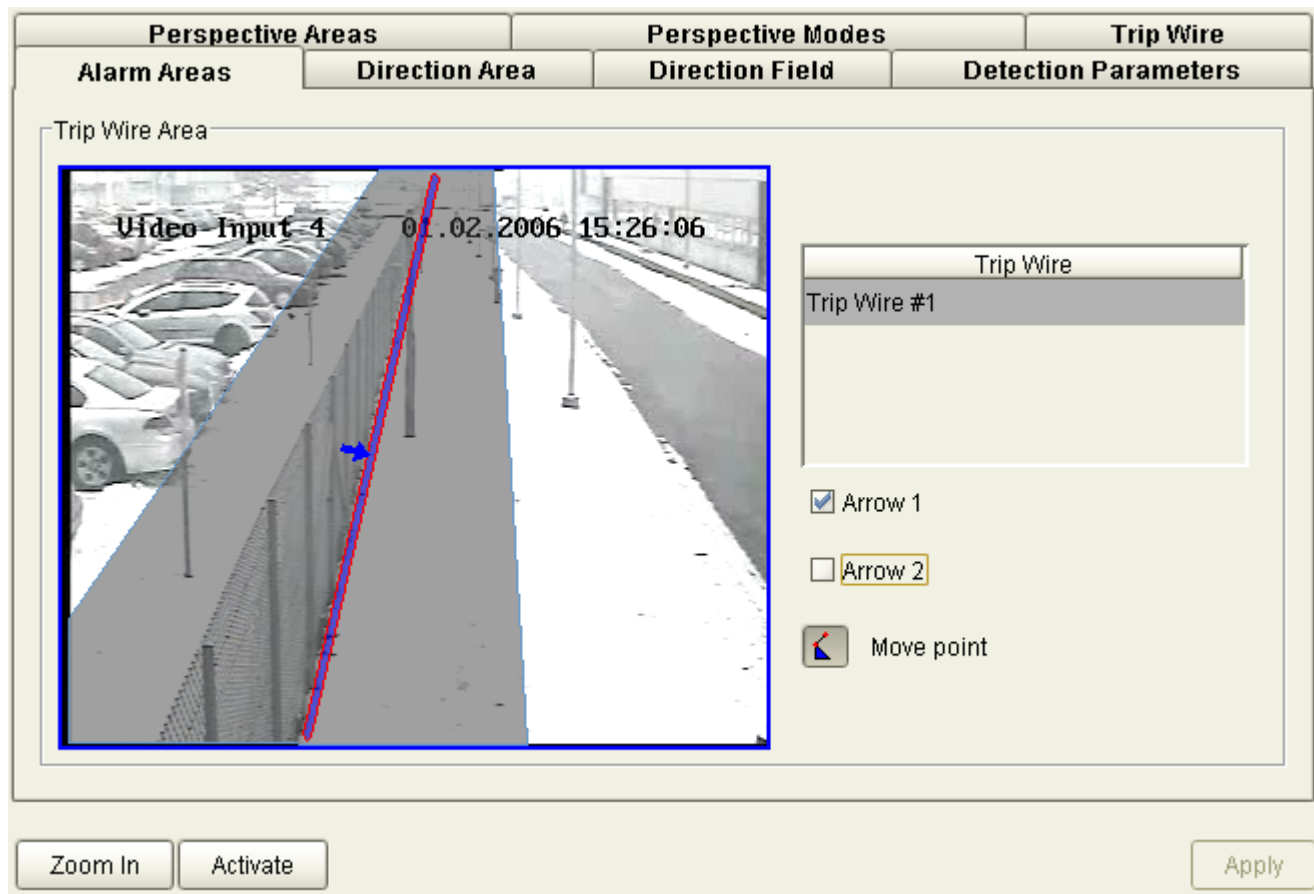
Fig. 82   Alarm program – "Alarm areas" tab

3. Select a trip wire from the list.
4. Select the direction of object movement.
5. Set the arrow(s) by ticking/unticking the appropriate checkbox(es).
6. You can enlarge or reduce the size of the image by clicking **Zoom In** and **Zoom Out**, respectively.
7. Use the toolbar icon to change the length of the arrow.
8. Click **Apply**.

Removing alarm areas

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2. Select the **Alarm Areas** tab.
3. Select a trip wire from the list.
4. Click on **Remove**.
5. Click **Apply**.

14.7.6   Examples of alarm area definition

CX
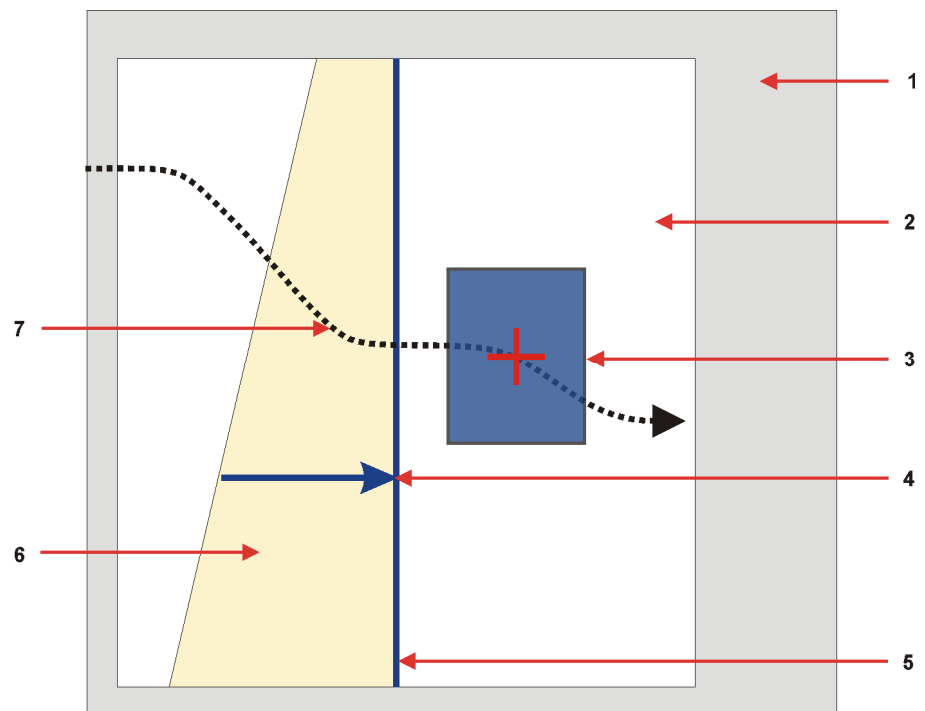
Fig. 83   Alarm area – Landscape perspective

1	**Live video**	
2	Perspective area	See Section: 14.7.1 Definition of perspective areas.
3	Object frame	See Section: 14.7.2 Defining the perspective mode.
4	Arrow	See Section: 14.7.5 Defining alarm areas.
5	Trip wire	See Section: 14.7.4 Defining trip wires.
6	Alarm area	See Section: 14.7.5 Defining alarm areas.
7	Path of motion	See Section: 14.6.1 Definition of global detection parameters.

Example
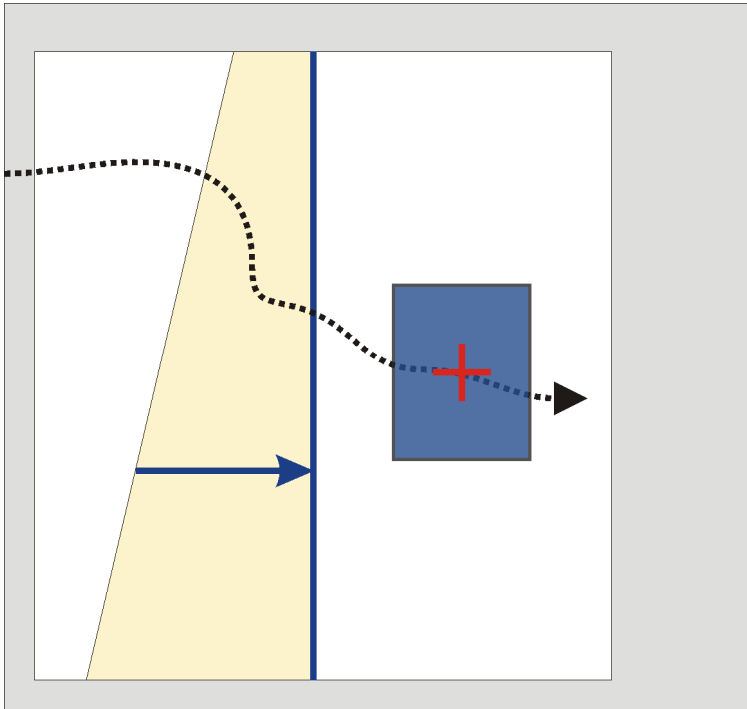
Explanation

The object centre has entirely crossed the alarm area and the trip wire in the predefined direction.

➔ An alarm is triggered.

Fig. 84   Alarm area – Landscape perspective
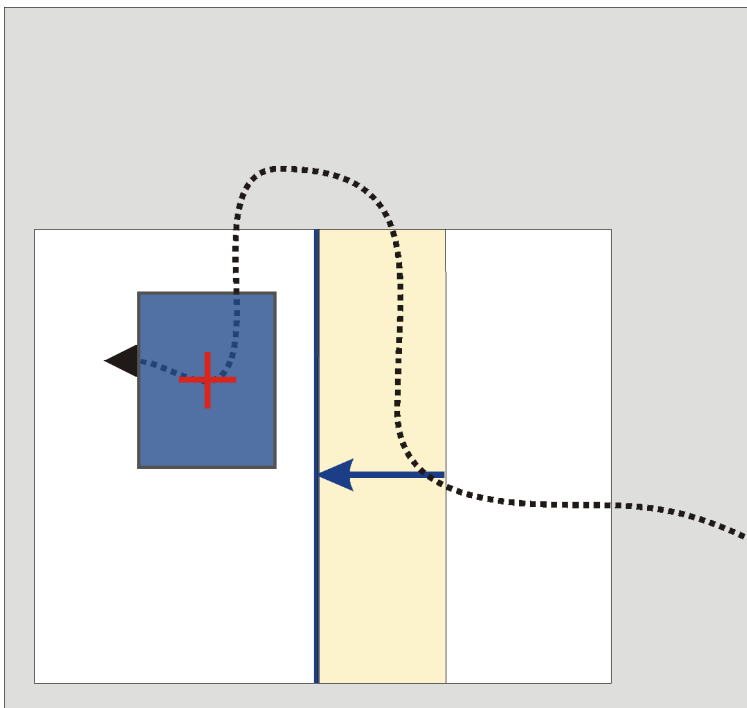
The object centre has left the perspective area and has not entirely crossed the alarm area and the trip wire.

➔ An alarm will **not** be triggered.

Fig. 85   Alarm area – Façade perspective

Example

Explanation

The object centre has not entirely crossed the alarm area.

➔ An alarm will **not** be triggered.
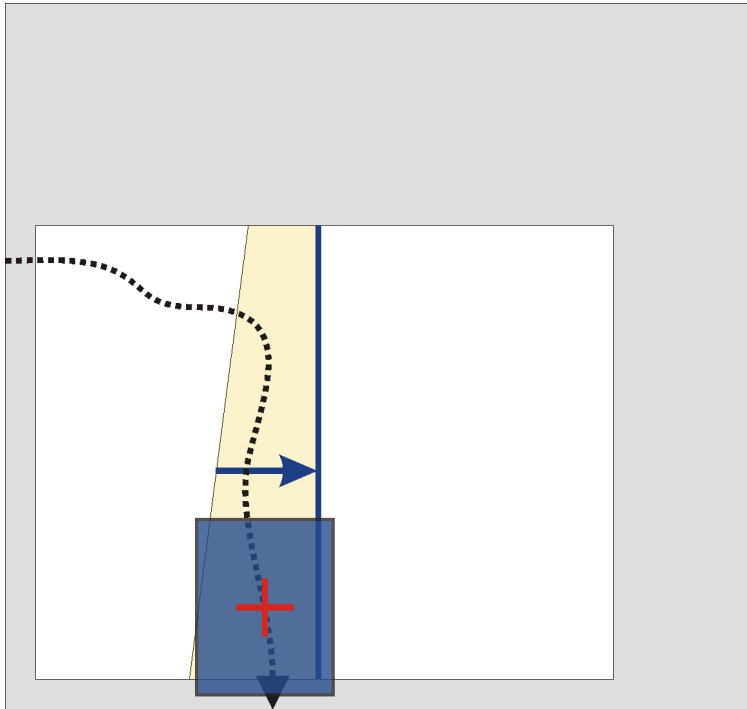
Fig. 86   Alarm area – Landscape perspective
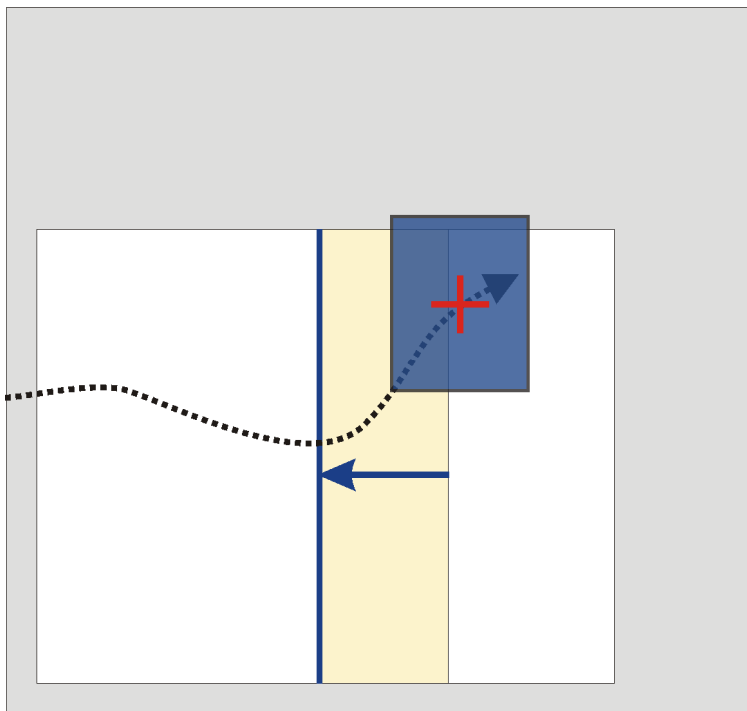
The object centre has not crossed the alarm area in the predefined direction.

➔ An alarm will **not** be triggered.

Fig. 87   Alarm area – Façade perspective

14.7.7 Defining the direction area

CX

Direction area

The direction area is an area within the perspective area where the formation and motion of objects is detected. The object movement to be detected is defined by the direction field. See Section: 14.7.8 Defining the direction field.

i
Only one direction area can be defined in each perspective area.

Defining the direction area

Prerequisites:

An alarm program has been defined. See Section: 14.4 Defining alarm programs.

A perspective area has been defined. See Section: 14.7.1 Definition of perspective areas.

A perspective mode has been defined. See Section: 14.7.2 Defining the perspective mode.

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2. Select the **Direction Area** tab.
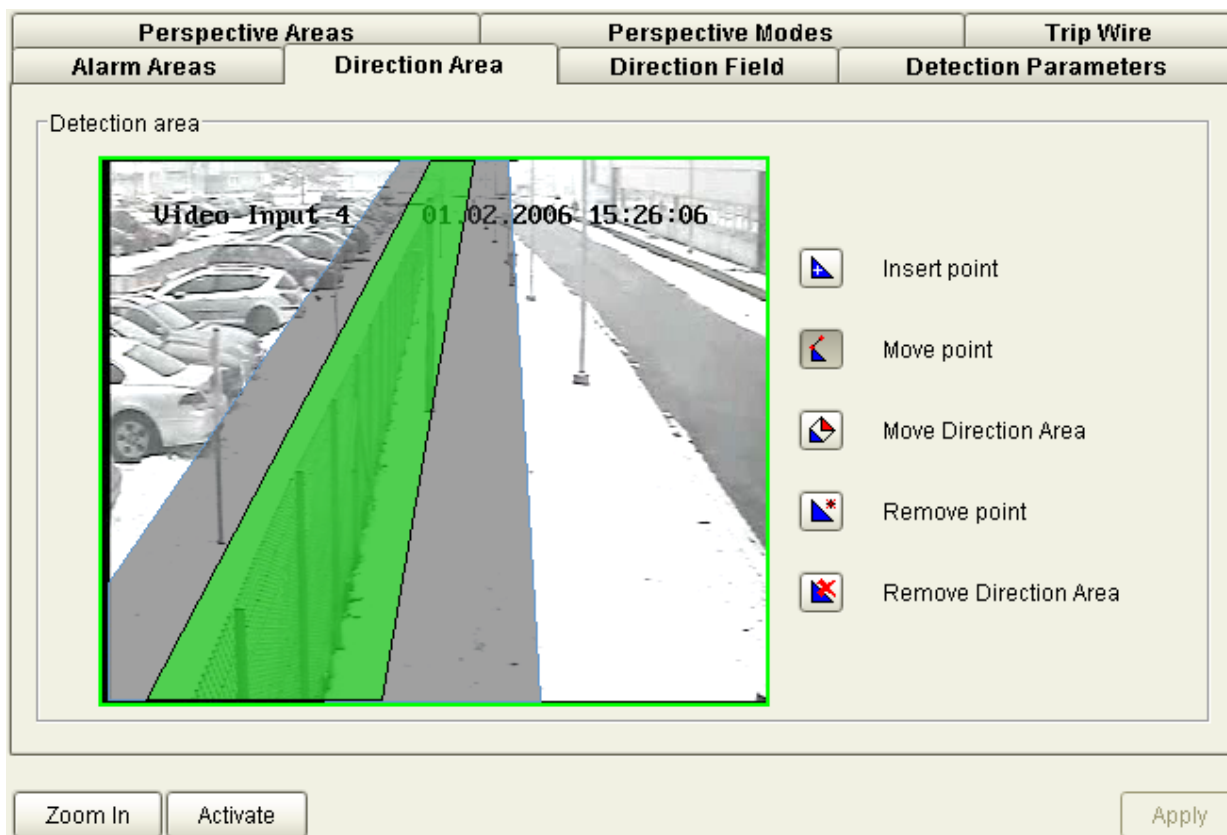
Fig. 88 Alarm program – "Direction Area" tab

3. You can enlarge or reduce the size of the image by clicking **Zoom In** and **Zoom Out**, respectively.

4. Use the toolbar icons to draw/alter a direction area.

5. Click **Apply**.

14.7.8   Defining the direction field

CX

Direction field

The direction field is an area in the direction area which defines through the arrows the direction of the object movement and the length of the distance an object located in the direction area has to cover in order to be detected and to trigger an alarm.

The direction field is defined by up to four arrows.

> **i**   One direction field can be defined for each direction area.
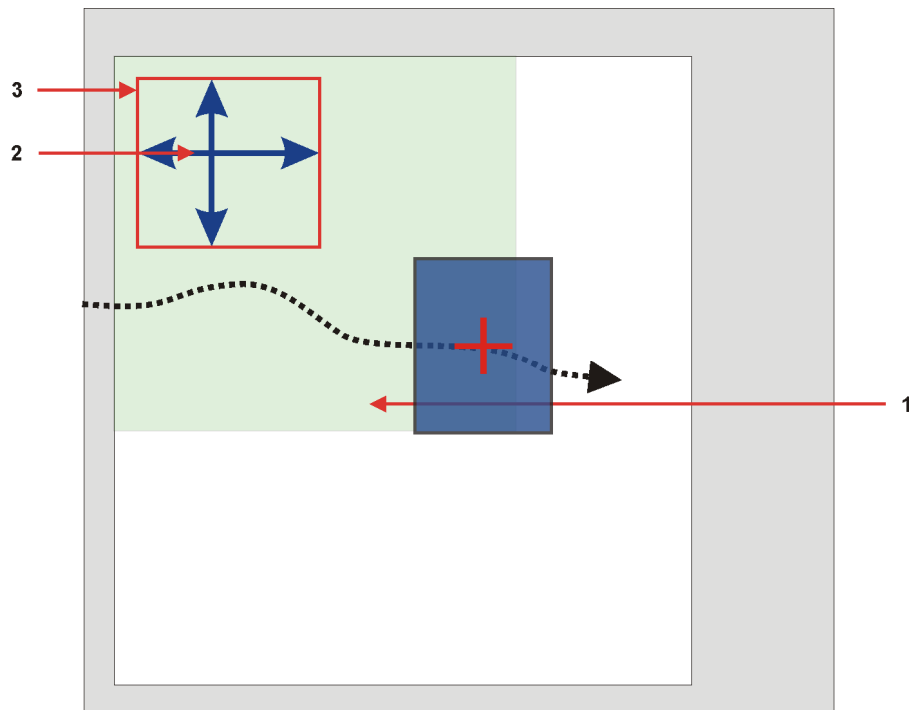
Fig. 89   Direction field – Landscape or façade perspective

1	Direction area	See Section: 14.7.7 Defining the direction area.
2	Arrows	See Section: 14.7.8 Defining the direction field.
3	Direction field	See Section: 14.7.8 Defining the direction field.

Defining the direction field

Prerequisites:

An alarm program has been defined. See Section: 14.4 Defining alarm programs.

A perspective area has been defined. See Section: 14.7.1 Definition of perspective areas.

A perspective mode has been defined. See Section: 14.7.2 Defining the perspective mode.

A direction area has been defined. See Section: 14.7.7 Defining the direction area.

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.

2. Select the **Direction Field** tab.
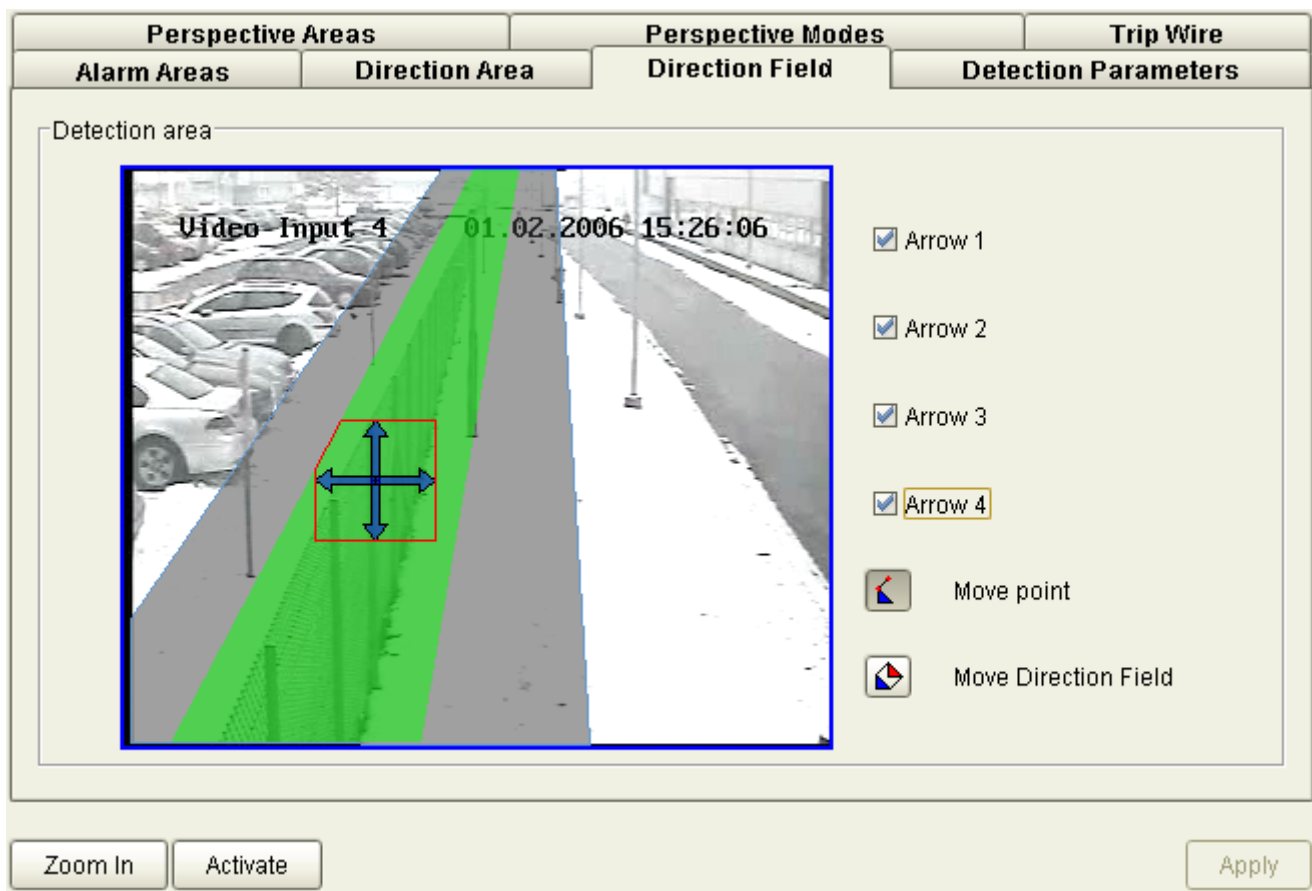
Fig. 90   Alarm program – "Direction Field" tab

3. Set the arrow(s) by ticking/unticking the appropriate checkbox(es).

4. Use the toolbar icons to edit the arrows.

    ➜ The direction area is indicated by a red frame.

5. Click **Apply**.

14.7.9 Examples of direction field definition

CX
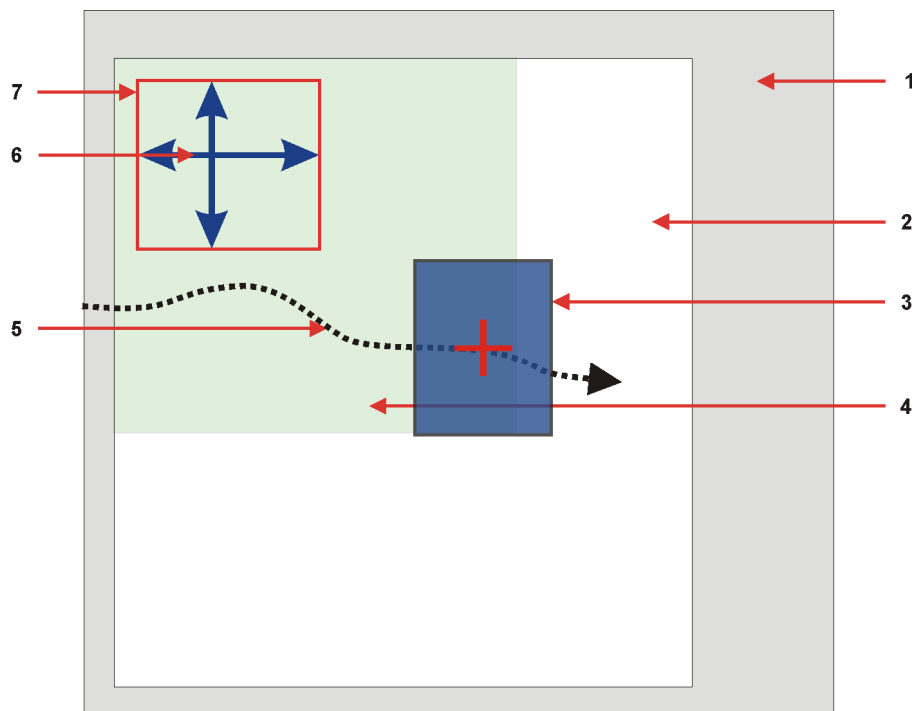
Fig. 91   Direction field – Landscape or façade perspective

1	**Live video**	
2	Perspective area	See Section: 14.7.1 Definition of perspective areas.
3	Object frame	See Section: 14.7.2 Defining the perspective mode.
4	Direction area	See Section: 14.7.7 Defining the direction area.
5	Path of motion	See Section: 14.6.1 Definition of global detection parameters.
6	Arrows	See Section: 14.7.8 Defining the direction field.
7	Direction field	See Section: 14.7.8 Defining the direction field.
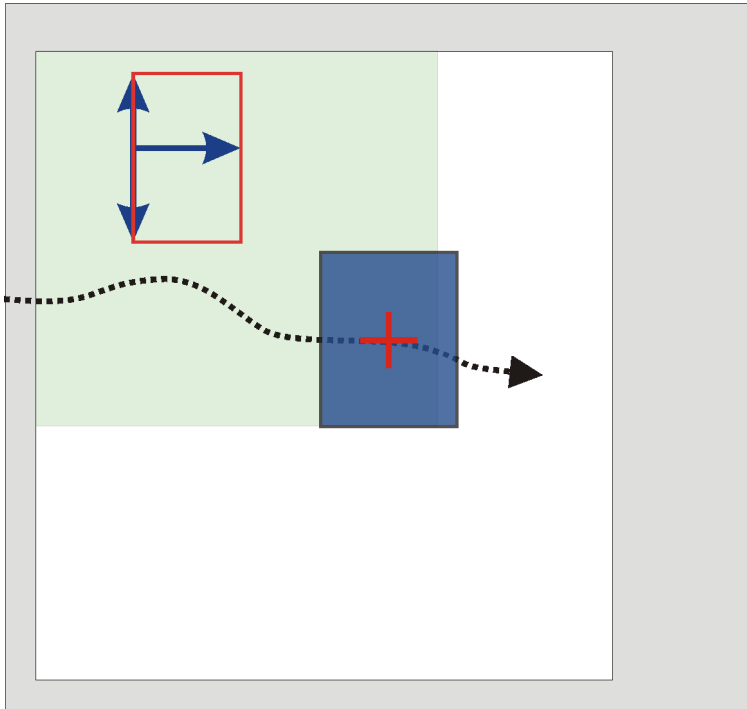
Configuring Enhanced Motion Detection

Example   **Explanation**

The object centre has crossed the direction area in the predefined direction and covered the specified distance.

➔ An alarm is triggered.
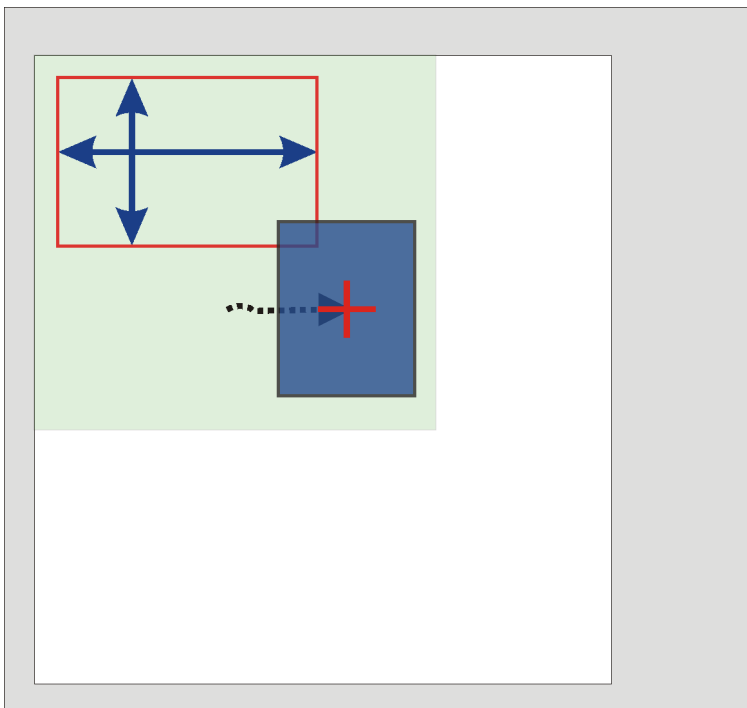
The object centre has crossed the direction area in the predefined direction but has not covered the specified distance.

➔ An alarm will **not be triggered yet**.

Example   **Explanation**
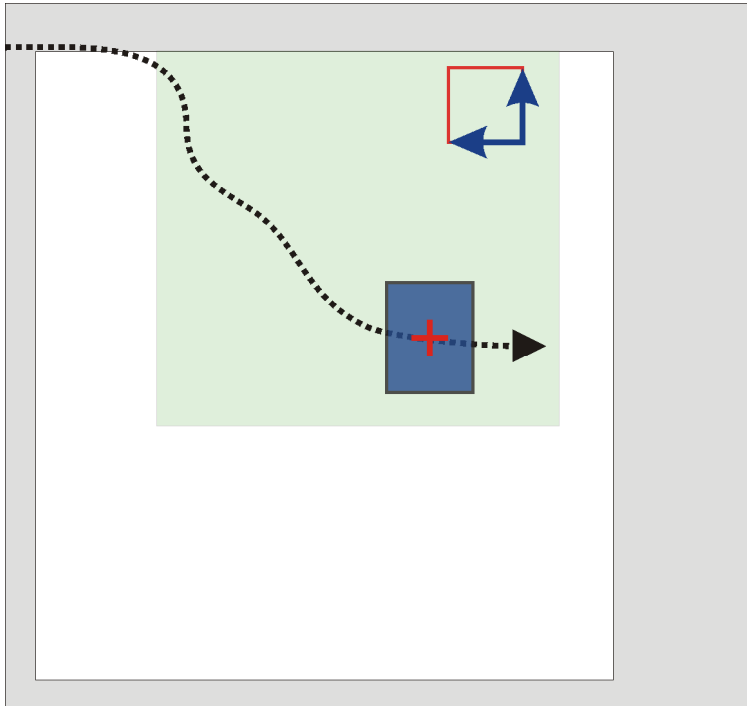
The object centre has not crossed the direction area in the predefined direction.
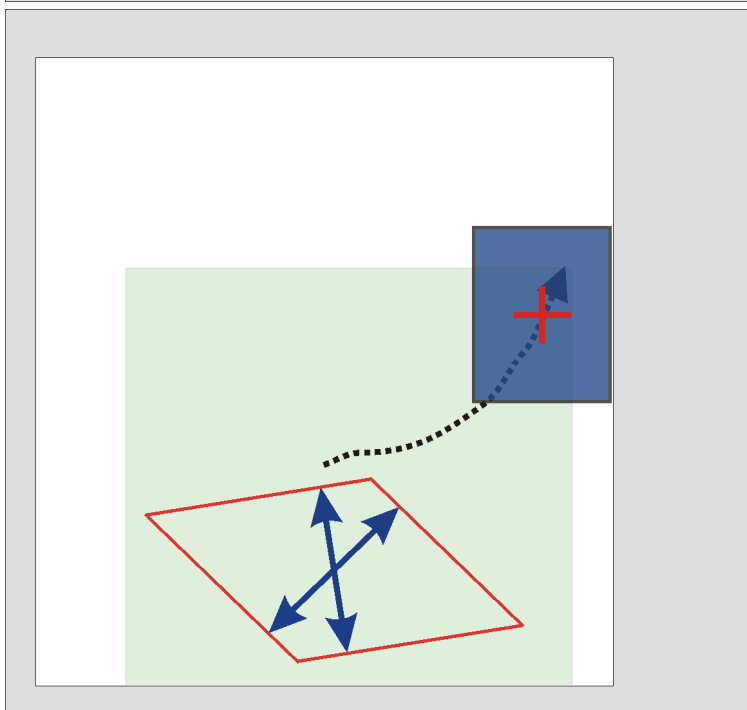
➔ An alarm will **not** be triggered.

The object centre has crossed the direction area in the predefined direction and covered the specified distance.

➔ An alarm is triggered.

14.7.10 Definition of program-specific detection parameters

CX

Program-specific detection parameters

Program-specific detection parameters are settings in the configuration software SISTORE CX Config for the detection of object movement that are valid for specific alarm programs.

Detection parameters of the Enhanced Motion Detection are: observation time, sensitivity, minimum object size and object velocity.

Observation time	Sensitivity	Min. object size	Max. object size	Velocity
The observation time is a detection parameter that determines the time between occurrence and detection of a motion. The longer the observation time the more precise is the object recognition.	The sensitivity is a detection parameter that determines the number of pixels that have to change within the live video to trigger an alarm. Sensitivity is specified in percentage. 100 % means that the sensitivity is very high, 0 % means that it is very low.	The minimum object size is a detection parameter that determines the minimum size an object must have to be detected. The minimum object size is indicated in percent to the object frame. Small objects or sporadic pixels can often be regarded as so called "noise".	The maximum object size is a detection parameter that determines the maximum size an object must have to be detected. The maximum object size is indicated in percent to the object frame.	The object velocity is a detection parameter that determines the max. speed at which an object can move to be detected.

Defining detection parameters

Prerequisite:

An alarm program has been defined. See Section: 14.4 Defining alarm programs.

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2. Select the **Detection Parameters** tab.

Fig. 92   Alarm program – "Detection Parameters" tab

| **i** | A suitable basic value for all detection parameters is 50. This value is set as the default value. |

3. Select a value for the **Observation Time** between **Very short** and **Very long**.
4. Select a value for the **Sensitivity** between **0 %** and **100 %**.
    ➔ The changes are visible immediately in the live video.
5. Select the **Sensitivity** such that there is no permanent noise in the live video.

| **i** | Noise in the live video that cannot be eliminated may also be dependent on the illumination conditions and on the type of camera used. |

6. Select a value for the **Minimal Object Size** between **0 %** and **100 %**.

Value	Example
0 %	Any object that is smaller or the same size as the object frame will be detected.
	With this setting, small objects such as for instance birds will also be detected.
50 %	The size of an object must be at least 50 % of the area within the object frame to be detected.
	With this setting, a person will only be detected if he or she covers at least 50 % of the area within the object frame. This also applies if the person is not walking upright.
	It is thus possible to exclude small animals from being detected.
100 %	In order to be detected, an object must fully cover the area within the object frame.
	A person will only be detected if his or her body height and width fully covers the object frame. This means that small persons, e.g. children, will not be detected.

Minimum object size reached:
- Detection is taking place.
- An alarm is triggered.
- The object frame and the course of motion are displayed in red.

Minimum object size not reached:
- Detection is taking place.
- An alarm will not be triggered.
- The object frame and the course of motion are displayed in white.

7. Select a value for the **Maximal Object Size** between **100 %** and **Unlimited**.

Value	Example
100 %	Any object that is smaller or the same size as the object frame will be detected. Objects that are larger than the object frame will not be detected.
1000 %	Any object that is up to 10 times the size of the object frame will be detected. Objects that are larger than this will not be detected.
Unlimited	There is no maximum object size. Objects of any size will be detected.

8. Select a value for the **Object Velocity** between **Very fast** and **Very slow**.

Value	Example
Very fast	**Car**
Fast	Bird
Normal	Cyclist
Slow	Sprint speed
Very slow	Walking speed

IMPORTANT	All velocity data refer to a person of approx. 1.70 m average height in the foreground of the live video.

9. Click **Apply**.

15 Configuring the detection of removed or left objects

CX

The function **Detection of removed or left objects** is a detection mode where objects that are removed from or left within the so-called alarm area are detected.

Detection modes are "Left objects" and "Removed objects".

Left objects	Removed objects
The detection mode "Left objects" defines when an object that is left within the alarm area will trigger an alarm. The detection is based on the following criteria: object size, pre-alarm time, alarm time, min. object size and max. object size. See Section: 15.7.5 Definition of program-specific detection parameters .	The detection mode "Removed objects" defines when an object that was removed from the alarm area will trigger an alarm. The detection is based on the following criteria: object size, pre-alarm time, alarm time, min. object size and max. object size. See Section: 15.7.5 Definition of program-specific detection parameters .

Configuration process

```
            ┌──────────────┐
            │    Start     │
            │ configuration│
            └──────┬───────┘
                   ▼
         ┌───────────────────┐
         │ Select video input│◄──────────┐
         └─────────┬─────────┘           │
                   ▼                      │
         ┌───────────────────┐           │
         │   Define alarm    │           │
         │     program       │           │
         └─────────┬─────────┘           │
                   ▼                      │
         ┌───────────────────┐           │
         │Define global alarm│           │
         │ program settings  │           │
         └─────────┬─────────┘           │
                   ▼                      │
         ┌───────────────────┐           │
         │ Define program-   │           │
         │ specific alarm    │           │
         │ program settings  │           │
         └─────────┬─────────┘           │
                   ▼              ┌───────────────┐
         ┌───────────────────┐    │ Disable alarm │
         │   Enable alarm    │    │    program    │
         │     program       │    └───────▲───────┘
         └─────────┬─────────┘            │
                   ▼                       │ No
         ┌───────────────────┐      ◄╲    │
         │ Observation for a │       ╱ ╲  │
         │ defined period of │──►  ╱Every╲
         │       time        │     ╲thing ╱
         └───────────────────┘      ╲ OK?╱
                                      ╲╱
                                       │ Yes
                                       ▼
                                ┌──────────────┐
                                │Configuration │
                                │  completed   │
                                └──────────────┘
```
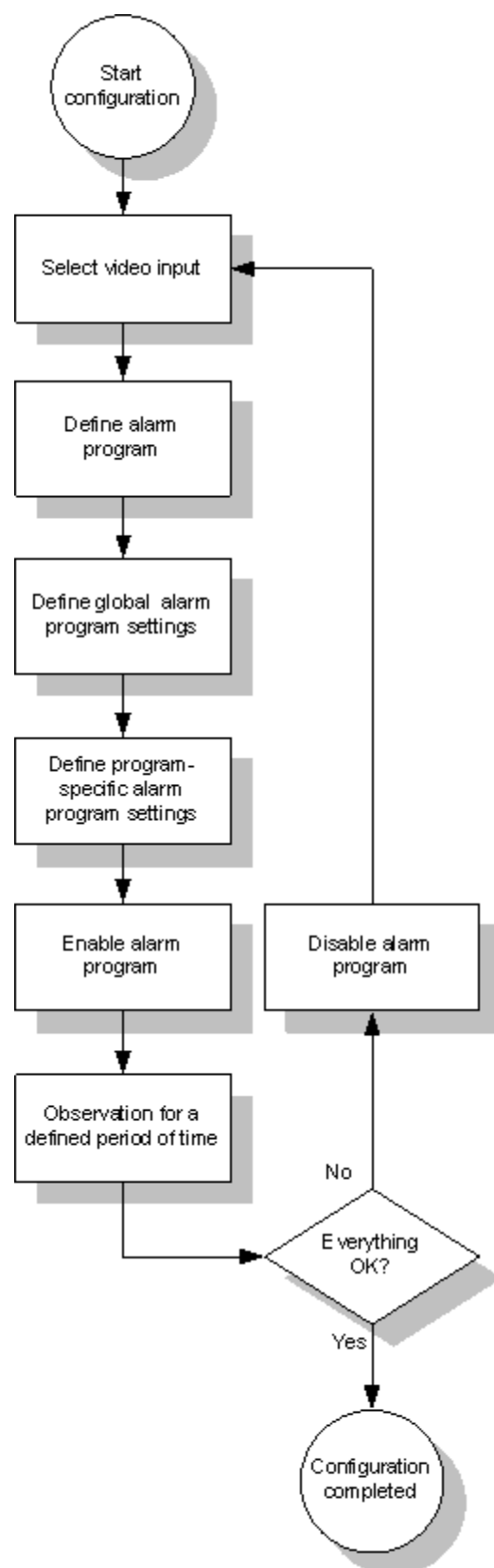
15.1   Colour of the symbol for Enhanced Motion Detection

CX

The symbol for the function "Detection of removed or left objects" in the tree structure provides the following information:

Grey		"Detection of removed or left objects" disabled
Red		"Detection of removed or left objects" enabled, main alarm
Green		"Detection of removed or left objects" enabled, no alarm triggered
Yellow		"Detection of removed or left objects" enabled, pre-alarm

15.2   Licence key entry

CX

1. In the tree view, navigate to the node **Video input**.
2. Click the **License key** button.
3. The **Input license** dialog box opens.
4. Enter the licence key using hyphens.
5. Click **OK**.
   ➔ The function "Detection of removed or left objects" has now been enabled and is ready for use.

15.3 Selecting the function "Detection of removed or left objects"

CX

Prerequisites:

The licence key has been entered.

An ODR operation mode has been selected. See Section: 8.1 Set operating mode.

A video input of a SISTORE device that supports the function "Removed or left objects" has been selected.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Video input**.
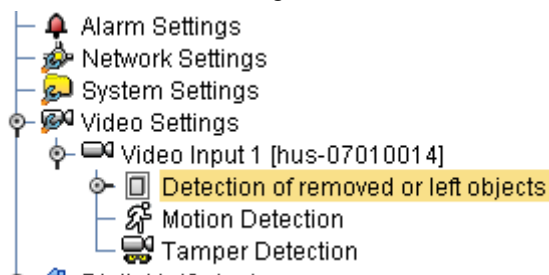
Fig. 93   Enhanced Motion Detection

3. Click on **Detection of removed or left objects**.

Siemens Building Technologies
Fire Safety & Security Products

15.4 Defining alarm programs

CX

Alarm program

An alarm program is a combination of detection parameters for a particular application.

It may be necessary to define different alarm programs for detecting objects during the day and at night.

i Up to four alarm programs can be defined for each video input.

1. Select **Detection of removed or left objects** in the tree structure. See Section: 15.3 Selecting the function "Detection of removed or left objects" .
2. Select the **Alarm programs** tab.
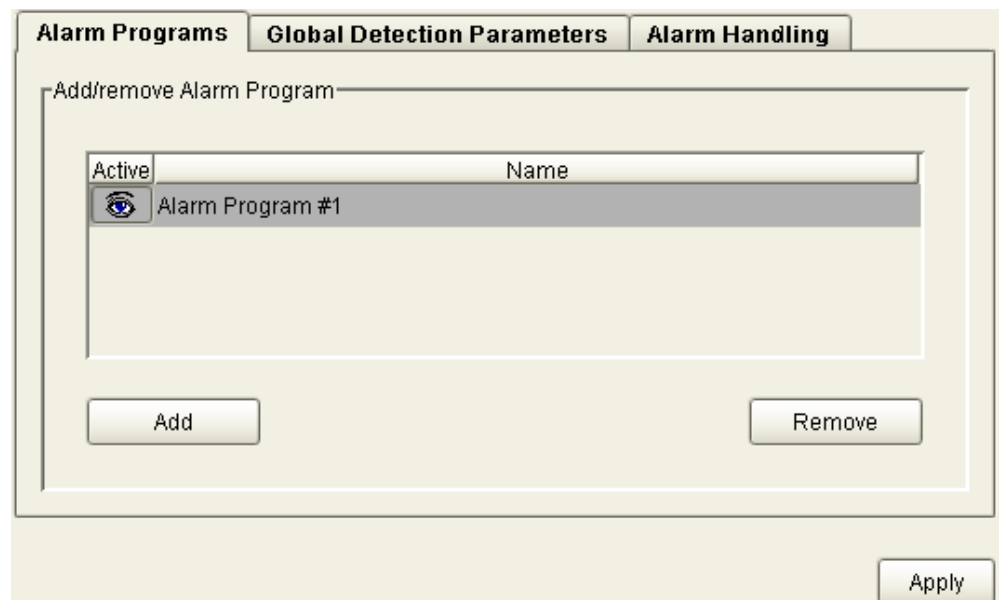
Fig. 94   Alarm program settings – "Alarm Programs" tab

3. Click **Add**.
   → The **Add Program** dialog box opens.
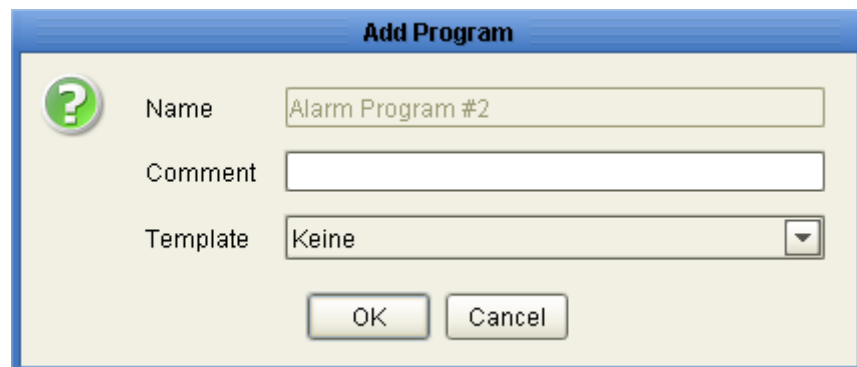
Fig. 95   Alarm program settings – "Add Program" dialog box

4. Add a comment on the alarm program in the **Comment** box.

5. To copy an alarm program, select a template from the **Template** list box.

6. Click **OK**.

➔ A new alarm program has now been defined.

7. Click **Apply**.

➔ The alarm program will now be listed under **Add/Remove Alarm Program**.

➔ The alarm program is also displayed in the device tree under **Detection of removed or left objects**.
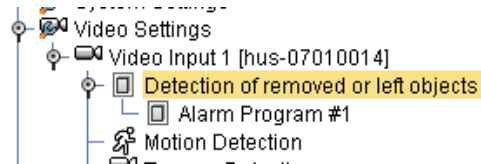
Fig. 96   Alarm program settings – Alarm Program

8. You can now set the alarm program parameters. See Section: 15.6 Global alarm program settings and Section: 15.7 Program-specific alarm program settings.

Removing alarm programs

1. Select **Detection of removed or left objects** in the tree structure. See Section: 15.3 Selecting the function "Detection of removed or left objects" .

2. Select the **Alarm programs** tab.

3. Select an alarm program from the list.

4. Click on **Remove**.

➔ The alarm program is now removed.

5. Click **Apply**.

➔ The alarm program will now be listed under **Add/Remove Alarm Program**.

➔ The alarm program is also displayed in the device tree under **Detection of removed or left objects**.

15.5   Activating an alarm program

CX

Prerequisite:

At least one alarm area for objects has been defined. See Section: 15.7.4 Define alarm areas.

There are several possibilities to activate an alarm program:

● Global alarm program settings

   – OR –

● Program-specific alarm program settings

Global alarm program settings

1.   Select **Detection of removed or left objects** in the tree structure. See Section: 15.3 Selecting the function "Detection of removed or left objects" .

2.   Select the **Alarm programs** tab.

3.   Select an alarm program from the list.

4.   Click on the "eye" under **Active**.

➔ The selected alarm program is now active. Alarms will be triggered as configured in the alarm program settings. See Section: 15.6 Global alarm program settings and Section: 15.7 Program-specific alarm program settings.

Program-specific alarm program settings

1.   Select **Detection of removed or left objects** in the tree structure. See Section: 15.3 Selecting the function "Detection of removed or left objects" .

2.   Select an alarm program. See Section: 15.4 Defining alarm programs.

3.   Make the desired program-specific settings.

4.   Click on **Activate**.

➔ The alarm program settings will be applied.

➔ The selected alarm program is now active. Alarms will be triggered as configured in the alarm program settings. See Section: 15.6 Global alarm program settings and Section: 15.7 Program-specific alarm program settings.

15.6   Global alarm program settings

15.6.1   Definition of global detection parameters

CX

Global detection parameters

Global detection parameters are settings in the configuration software SISTORE CX Config for the detection of objects that are valid for all alarm programs.

Global detection parameters for the detection of removed or left objects are the object display mode.

Object display mode

The object display mode specifies which objects will be displayed with a frame around them.

Object display modes are: the object frames of removed and/or left objects and the object frames of all detected objects.

Object frames of removed and/or left objects	Object frames of all detected objects
Detected objects that will trigger an alarm based on the detection parameters, will be highlighted by an object frame.	All objects that were detected will be highlighted by an object frame, regardless of the detection parameters.

Meaning of the colour of object frames

White	The object is not compliant with the detection parameters set or it is outside the alarm area and will therefore not trigger an alarm. See Sections: 15.7.5 Definition of program-specific detection parameters and 15.7.4 Define alarm areas.
Yellow	The object has been detected as an object and is in pre-alarm condition. See Section: 15.7.5 Definition of program-specific detection parameters .
Red	The object has been detected as an object and is in alarm condition. See Section: 15.7.5 Definition of program-specific detection parameters .

Definition of global detection parameters

Prerequisite:

An alarm program has been defined. See Section: 15.4 Defining alarm programs.

1. Select **Detection of removed or left objects** in the tree structure. See
    Section: 15.3 Selecting the function "Detection of removed or left objects" .
2. Select the **Global Detection Parameters** tab.
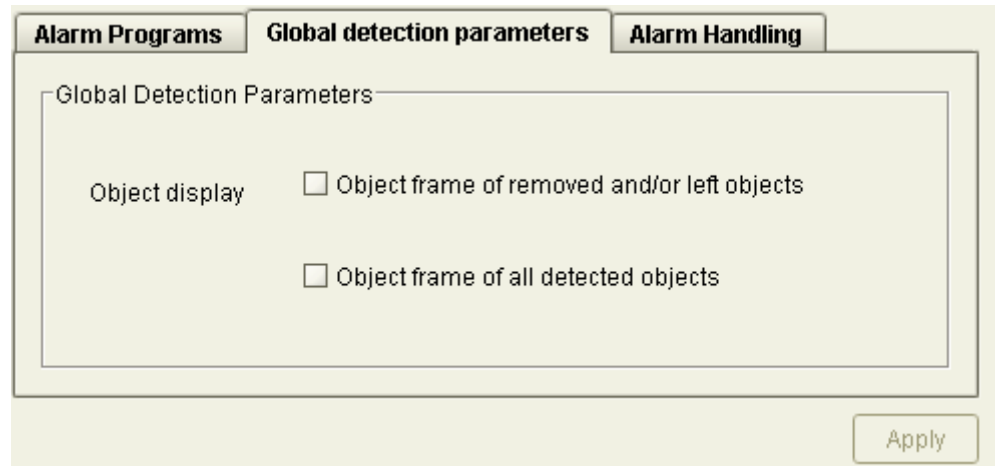
Fig. 97   Alarm program settings – "Global Detection Parameters" tab

3. Mark the checkbox **Object frame of removed and/or left objects** and/or
    Object frame of all detected objects.
4. Click **Apply**.

15.6.2 Definition of the alarm handling

CX

Alarm handling

Alarm handling is a software setting/mode which handles alarm transmission.

Digital output

A digital output is an output on a device where signal transmitters can be connected.

External signal transmitters, such as audible alarms, lamps, door sensors or light barriers, can receive a signal from the device via a relay.

Definition of the alarm handling

Prerequisite:

An alarm program has been defined. See Section: 15.4 Defining alarm programs.

1.   Select **Detection of removed or left objects** in the tree structure. See Section: 15.3 Selecting the function "Detection of removed or left objects" .
2.   Select the **Alarm Handling** tab.

Fig. 98   Alarm program settings – "Alarm Handling" tab

3.   Select a digital output for both alarm and pre-alarm from the appropriate list box.
4.   Click **Apply**.

15.7   Program-specific alarm program settings

CX

Program-specific settings are made individually for each alarm program.

Program-specific settings are:

- Perspective area
- Perspective mode
- Alarm area - object
- Program-specific detection parameters

15.7.1   Definition of perspective areas

CX

Perspective area

The perspective area is an area within the live video where the formation and/or motion of objects is detected and/or tracked.

The user defines two object sizes within the perspective area: one in the foreground and one in the background. In doing so, the size differences in the live video that result from the perspective are analysed correctly.

ℹ️   Up to four perspective areas can be defined for each live video.

Definition of perspective areas

Prerequisite:

An alarm program has been defined. See Section: 15.4 Defining alarm programs.

1.   Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2.   Select the **Perspective Areas** tab.

Fig. 99   Alarm program – "Perspective Areas" tab

3.   Click **Add**.
4.   Select a perspective area from the list.
5.   Use the toolbar to draw or change a perspective area.
6.   Click **Apply**.

Removing perspective areas

1.   Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2.   Select the **Perspective Areas** tab.
3.   Select a perspective area from the list.
4.   Click on **Remove**.

   ➜ The perspective area no longer appears in the list.

5.   Click **Apply**.

Show/hide perspective areas

This function provides more clarity when creating or changing perspective areas.

1.   Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2.   Select the **Perspective Areas** tab.
3.   Select a perspective area from the list.
4.   Click on the "eye" to show or hide the perspective area.

   ➜ The perspective area now either disappears or is displayed.

15.7.2   Defining the perspective mode

CX

Perspective mode

Perspective modes are landscape perspective and façade perspective.

In the perspective mode it can be determined in which perspective an object has to appear within a predefined perspective area to be detected. The decisive factor is the distance between object and camera.

Landscape perspective	Façade perspective
The landscape perspective is a perspective mode.	The façade perspective is a perspective mode.
With the landscape perspective the object size is evaluated in a predefined perspective area of the live video. The object size in the live video depends on the object's distance to the camera. With the landscape perspective the object size in the live video changes noticeably.	With the landscape perspective the object size is evaluated in a predefined perspective area of the live video. The object size in the live video depends on the object's distance to the camera. With the façade perspective the object size in the live video rarely changes.
→ Two object frames of different sizes appear in the perspective area. Both object frames have the same aspect ratio. 	→ Two object frames of the same size appear in the perspective area.

Defining the perspective mode

Prerequisites:

An alarm program has been defined. See Section: 15.4 Defining alarm programs.

A perspective area has been defined. See Section: 15.7.1 Definition of perspective areas.

1. Select an alarm program in the tree structure. See Section: 14.4 Defining alarm programs.
2. Select the **Perspective Modes** tab.

Fig. 100   Alarm program – "Perspective Modes" tab

3. Select the **perspective area** for which you want to define a perspective mode.
4. Activate either **Landscape Perspective** or **Façade Perspective**.
5. Click **Apply**.
6. Match the size of the object frame to the perspective mode. See
    Section: 15.7.3 Matching the size of the object frame to the perspective mode.

15.7.3   Matching the size of the object frame to the perspective mode

CX

Object frame

The object frame is the rectangular demarcation of an object within the live video. See Section: 15.6.1 Definition of global detection parameters.

1.   Select an alarm program in the tree structure. See Section: 15.4 Defining alarm programs.

2.   Select the **Perspective Modes** tab.

3.   Place an object in the monitored area.

4.   You can enlarge or reduce the size of the image by clicking **Zoom In** and **Zoom Out**, respectively.

5.   Use the toolbar icons to match the size of the object frame in the live video to the actual object size.

> **i** The width-to-height ratio of the light-coloured object frame is automatically matched to the dark-coloured object frame and can therefore not be changed.

6.   Click **Apply**.

7.   Determine the minimum and maximum size an object must be in order to be detected. See Section: 15.7.5 Definition of program-specific detection parameters .

15.7.4   Define alarm areas

CX

Alarm area

The alarm area for objects is a defined area in the live video where removed and/or left objects are detected.

If an object is removed from or left in an alarm area, an alarm will be triggered. See Section: 15.7.5 Definition of program-specific detection parameters .
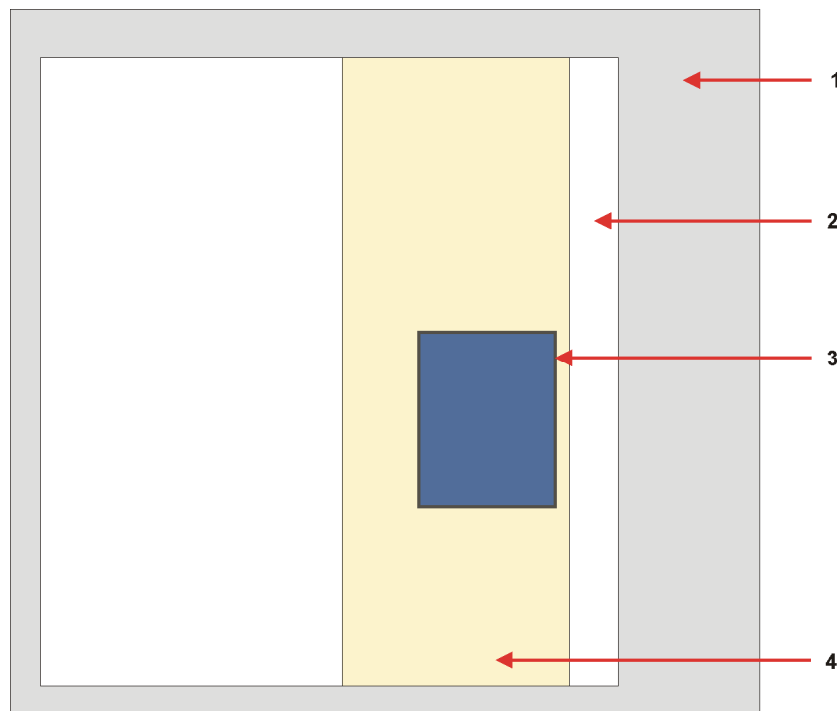
Fig. 101   Alarm area – Landscape perspective or façade perspective

1	**Live video**	
2	Perspective area	See Section: 15.7.1 Definition of perspective areas.
3	Object	See Section: 15.7.2 Defining the perspective mode and Section: 15.7.3 Matching the size of the object frame to the perspective mode.
4	Alarm area	See Section: 15.7.4 Define alarm areas.

i   Up to eight alarm areas can be defined.

Define alarm areas

Prerequisites:

An alarm program has been defined. See Section: 15.4 Defining alarm programs.

A perspective area has been defined. See Section: 15.7.1 Definition of perspective areas.

A perspective mode has been defined. See Section: 15.7.2 Defining the perspective mode.

1. Select an alarm program in the tree structure. See Section: 15.4 Defining alarm programs.

2. Select the **Alarm areas - objects** tab.
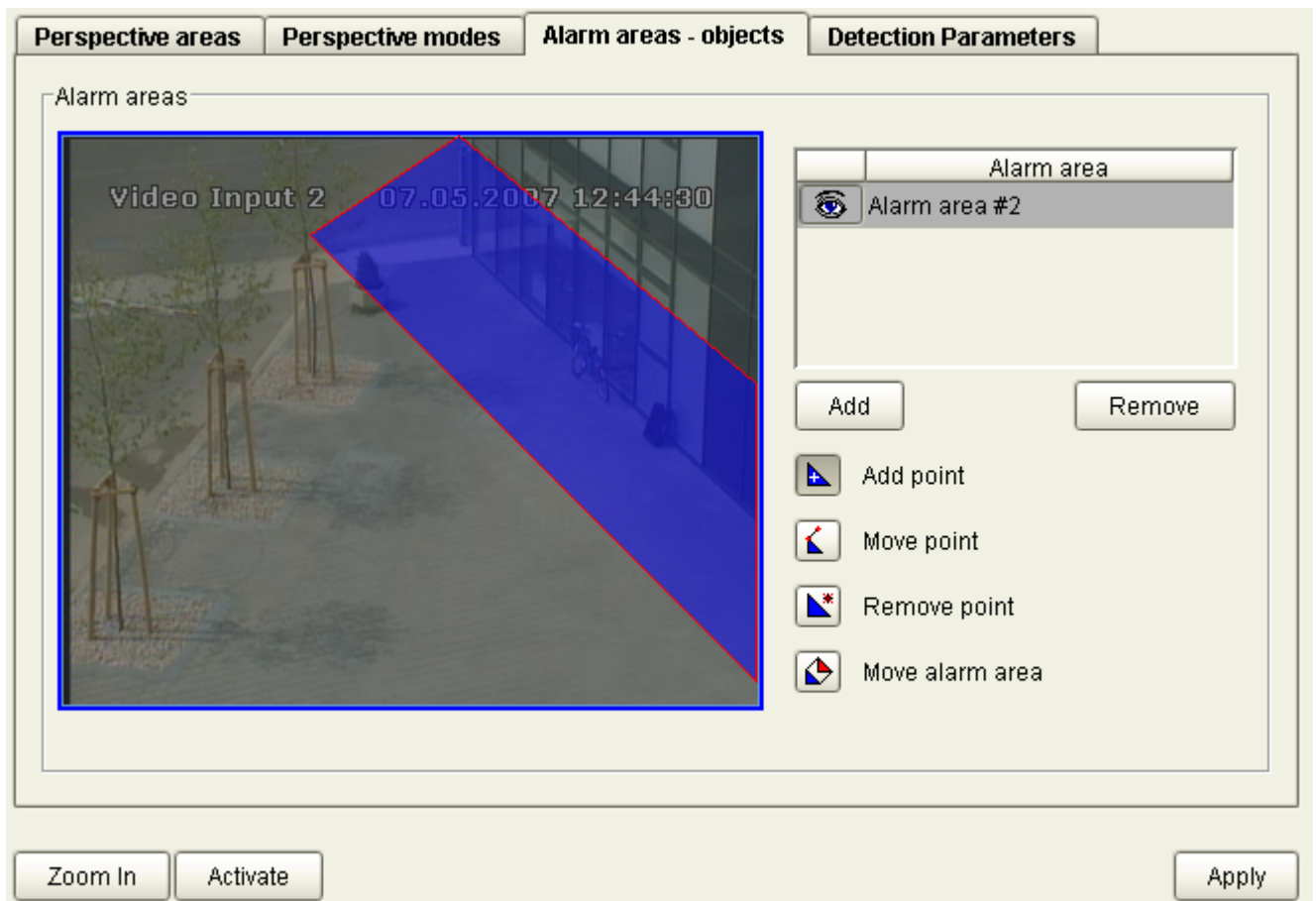
Fig. 102   Alarm program – "Alarm areas" tab

3. Click **Add**.

4. Select an alarm area from the list.

5. You can enlarge or reduce the size of the image by clicking **Zoom In** and **Zoom Out**, respectively.

6. Use the toolbar icons to draw/change the alarm areas.

7. Click **Apply**.

Remove alarm areas

1. Select an alarm program in the tree structure. See Section: 15.4 Defining alarm programs.

2. Select the **Alarm areas - objects** tab.

3. Select an alarm area from the list.

4. Click on **Remove**.

5. Click **Apply**.

Show/hide alarm areas

1. Select an alarm program in the tree structure. See Section: 15.4 Defining alarm programs.

2. Select the **Alarm areas - objects** tab.

3. Select an alarm area from the list.

173

4. Click on the "eye" to show or hide the alarm area.

   ➔ The alarm area now either disappears or is displayed.

Change alarm area ID

1. Double-click on an alarm area in the list.

   ➔ The **Input** dialog will open.

2. Enter a new ID in the input field.

3. Click **OK**.

15.7.5 Definition of program-specific detection parameters

CX

Program-specific detection parameters

Program-specific detection parameters for removed and/or left objects are: pre-alarm time, alarm time, min. object size and max. object size.

There are cases in which it is not recommendable that an alarm be triggered as soon as an event (an object was removed or left) is detected, but the scene be observed and evaluated for a certain period of time (pre-alarm time). If the event persists for the entire pre-alarm time, a pre-alarm may be generated. When a pre-alarm is triggered, a monitor can be activated for instance. If the event persists for the entire alarm time, an alarm may be generated as a consequence. When an alarm is triggered, recording can be started for instance.

Pre-alarm time	Alarm time	Min. object size	Max. object size
The pre-alarm time is a detection parameter that determines the time between occurrence of an event and the triggering of the pre-alarm. The pre-alarm time is at most as long as the alarm time. The colour of the object frame is yellow.	The alarm time is a detection parameter that determines the time between the occurrence of an event and the triggering of the alarm. The alarm time is at least as long as the pre-alarm time. The colour of the object frame is red.	The minimum object size is a detection parameter that determines the minimum size an object must have to be detected. The minimum object size is indicated in percent to the object frame. Small objects or sporadic pixels can often be regarded as so called "noise".	The maximum object size is a detection parameter that determines the maximum size an object must have to be detected. The maximum object size is indicated in percent to the object frame.
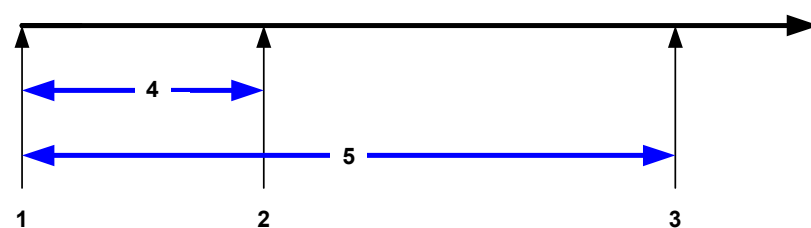
1	Event (an object was removed or left)
2	Pre-alarm (possible action: e.g. connection of a monitor)
3	Alarm (possible action: e.g. start of recording)
4	Pre-alarm time
5	Alarm time

Defining detection parameters

Prerequisite:

An alarm program has been defined. See Section: 15.4 Defining alarm programs.

1. Select an alarm program in the tree structure. See Section: 15.4 Defining alarm programs.

2. Select the **Detection Parameters** tab.
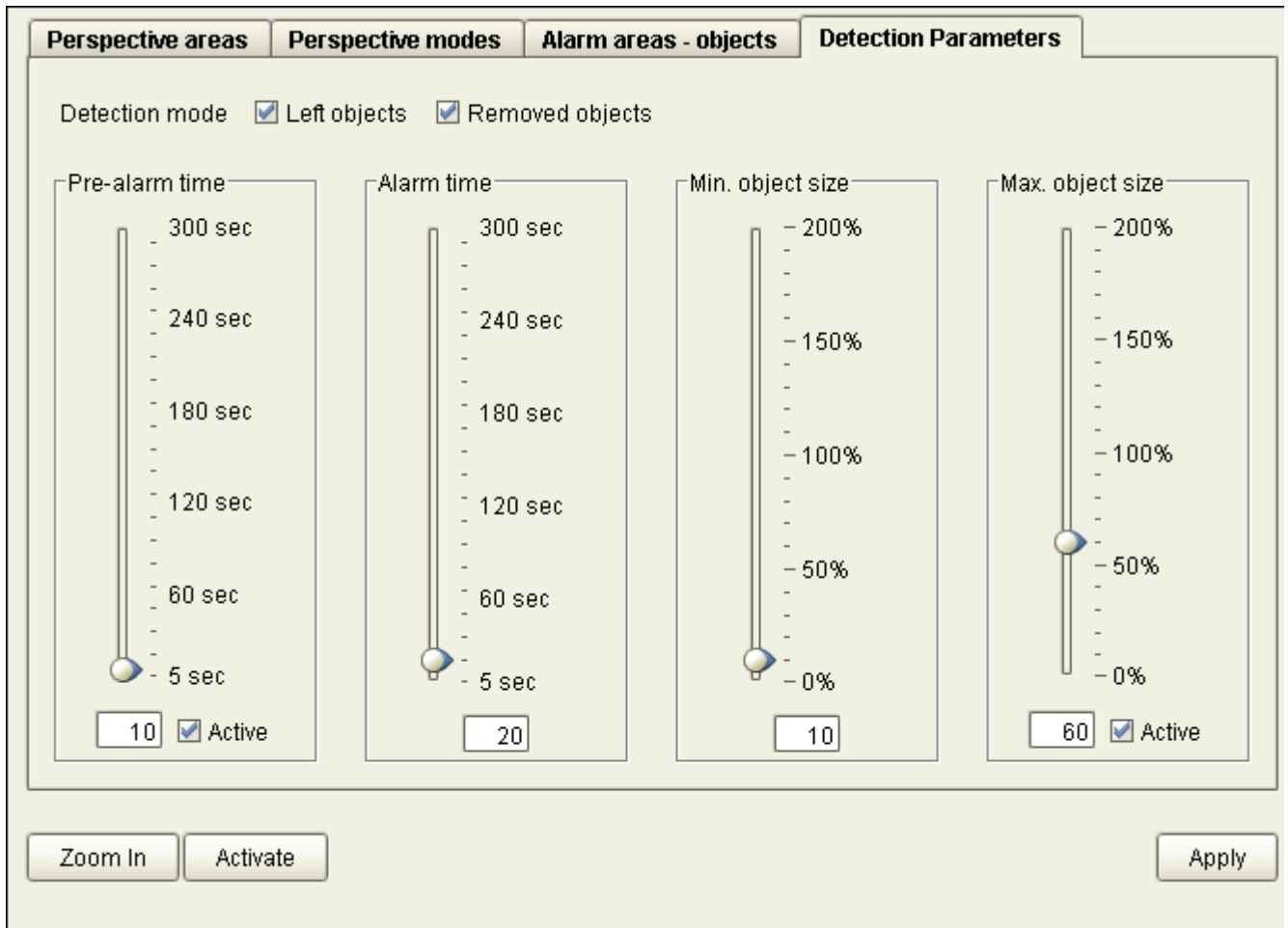
Fig. 103   Alarm program – "Detection Parameters" tab

3. Mark either or both checkboxes **Left objects** / **Removed objects**. See Section: 15 Configuring the detection of removed or left objects.

> **i** If the detection modes **Left objects** and **Removed objects** are activated simultaneously and an object is removed, then an alarm of type "left object" will be generated.

4. Set the **Pre-alarm time** between **5 sec** and **300 sec**.

5. To deactivate the pre-alarm time untick the **Active** checkbox.

6. Set the **Alarm time** between **5 sec** and **300 sec**.
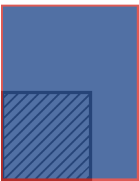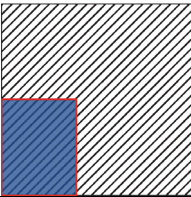
> **i** The alarm time must be at least as long as the pre-alarm time. The slide control for the alarm time will be adjusted automatically.
>
> The pre-alarm time and the alarm time may slightly differ from the values set, depending on the motion in the live video.
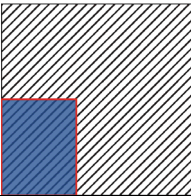
7. Select a value for the **Min. object size** between **0 %** and **200 %**.

> **i** The actual object size may slightly differ from the detected object size.

Value	Example
0 %	Every object will be detected irrespective of its size.
50 %	In order for an object to be detected, its height and width must be at least 50 % of the defined size of the object frame. Thus, small bags or other small objects can be excluded from being detected.
200 %	In order for an object to be detected, its height and width must be at least 200 % of the defined size of the object frame. This setting can be used for instance to detect cars that are not parked correctly.

8. Select a value for the **Max. object size** between **0 %** and **200 %**.

Value	Example
0 %	No object will be detected.
50 %	In order for an object to be detected, its height and width must not exceed 50 % of the defined size of the object frame. This setting can be used for instance to detect only small objects.
200 %	In order for an object to be detected, its height and width must not exceed 200 % of the defined size of the object frame. With this setting, parked cars will not be detected.

9. To deactivate the max. object size, untick the **Active** checkbox.

> **i** The maximum object size must not be smaller than the minimum object size. The slide control for the maximum object size will be adjusted automatically.

10. Click **Apply**.

16 Configuring tamper detection

CX FDV

Tamper detection is used to determine whether a camera was moved or covered. If so, this means that the camera was **tampered with**.

When configuring tamper detection, you first define a detection area in the video image (specific section of the video image). Variations in the image will be recognised in this area and may then trigger an **alarm**, depending on the **detection parameters**.

You can now select tamper detection as an event type for rule configuration. See Section: 18 Rule configuration.

i

If the tamper detection function is activated on the Video Fire Controller (see Section: 16.5 Activating / deactivating tamper detection) and the camera is tampered with, an alarm will be reported via **FDnet IN 4** to the fire alarm control panel (see Fig. 13). More detailed information on the evaluation and configuration of the alarm message by the fire alarm control panel can be found in the Configuration Manual and in the user manual for the fire alarm control panel.

The message types of CCTV and fire alarms may belong to different alarm classes and have different priorities.

Tamper detection alarms can only be acknowledged via the CCTV system (see Section: 16.6 Acknowledging tamper alarms).

16.1 Configuration of tamper detection

CX FDV

- Select the detection area
- Define the detection parameters
- Activate tamper detection

16.2 The colour of the tamper detection icon

CX FDV

The symbol for the motion detection in the tree structure provides the following information:

No colour		Tamper detection deactivated
Red		Tamper detection activated, tampering detected, alarm triggered
Yellow		Initialization of the tamper detection function
Green		Tamper detection activated, no tampering detected, no alarm

16.3 Defining the detection area (tamper detection)

CX FDV

ℹ️ When configuring tamper detection, a detection area has to be defined.

Prerequisite:

A video input of a SISTORE device which supports the tamper detection function has been selected.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Video input**.
   See Section: 8.4 Configuring video inputs.
3. Click on **Tamper Detection**.
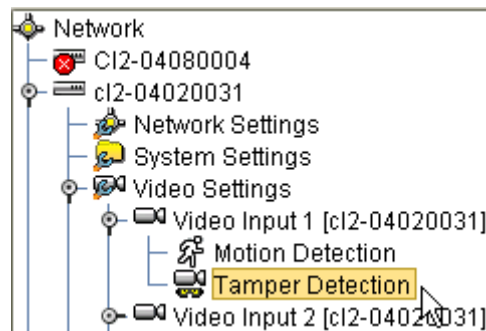
4. Select the **Detection area** tab.
   ➔ The live video of the camera for which you want to determine a detection area is now displayed.
5. Add a new detection area using the icons on the right of the live video.
6. Using these icons, you can freely configure the detection area and position it anywhere in the live video. You can add and insert further points and move existing points within the detection area.
7. Click **Apply**.

ℹ️ You can stipulate several detection areas per video input (live video).

ℹ️ The detection area for tamper detection should always be located in an area of the image where few changes occur and where many invariable edges are visible. Variations in the image, caused by tampering with the camera (camera was moved or covered), can thus easily be detected.

16.4 Defining the detection parameters (tamper detection)

CX FDV

> ℹ️ When you switch to configuration mode, tamper detection is automatically activated. First deactivate all associated rules in the SISTORE CX Client so that no recordings are accidentally triggered. It is not possible to suppress the alerts sent to the video management system IVM.

Prerequisite:

At least one detection area has been defined. See Section: 16.3 Defining the detection area (tamper detection).

1.   Select the detection areas of the live video for which you want to set the detection parameters. If you have determined several detection areas in one image, then the same parameters will apply to all these areas.

2.   Set the following parameters in the **Detection parameters** tab:

> ℹ️ The value entered for the observation time must be a multiple of 40.

Fig. 104   "Detection parameters" tab

Sensitivity	The percentage of changes in the images or the image area that must occur before an alarm is triggered. The transmitted images are evaluated for a certain time period. If the changes during this period are minimal, then no alarm will be generated.
	Basically: The higher the value, the lower the sensitivity for tamper detection.
	Set the control to the lowest setting at which the image noise no longer triggers the motion detection but tampering is still reliably detected under all occurring lighting conditions.
Observation time	Period of time during which a change in the image should be detected.
Initialization	Indicates the initialization progress. Initialization following a change of parameters takes about 2 minutes. The tamper detection function is active when the initialization is completed.

3.   Click **Apply**.

16.5 Activating / deactivating tamper detection

CX FDV

Prerequisites:

At least one detection area has been defined. See Section: 16.3

Defining the .

The detection parameters for the detection areas have been defined. See Section: 16.4 Defining the detection parameters (tamper detection).

Activating the tamper detection
1. Tick the checkbox **Activate** in the **Detection area** tab.
2. Click **Apply**.
    ➔ The detection area is now active and the detection parameters you have defined will be applied. If the camera is tampered with, this may cause an alarm to be triggered.
    ➔ You can now select tamper detection as an event type for rule configuration. See Section: 18 Rule configuration.

Deactivating the tamper detection
1. Untick the checkbox **Activate** in the **Detection area** tab.
2. Click **Apply**.

16.6 Acknowledging tamper alarms

CX FDV

> The alarm acknowledgement described below is only used for service purposes. In normal mode, alarms are recorded and acknowledged via the IVM system.

Prerequisites:

At least one detection area has been defined. See Section: 16.3

Defining the .

The tamper detection function is active and alarms have been triggered. See Section: 16.5 Activating / deactivating tamper detection.

1. Click the **Acknowledge alarm** button.
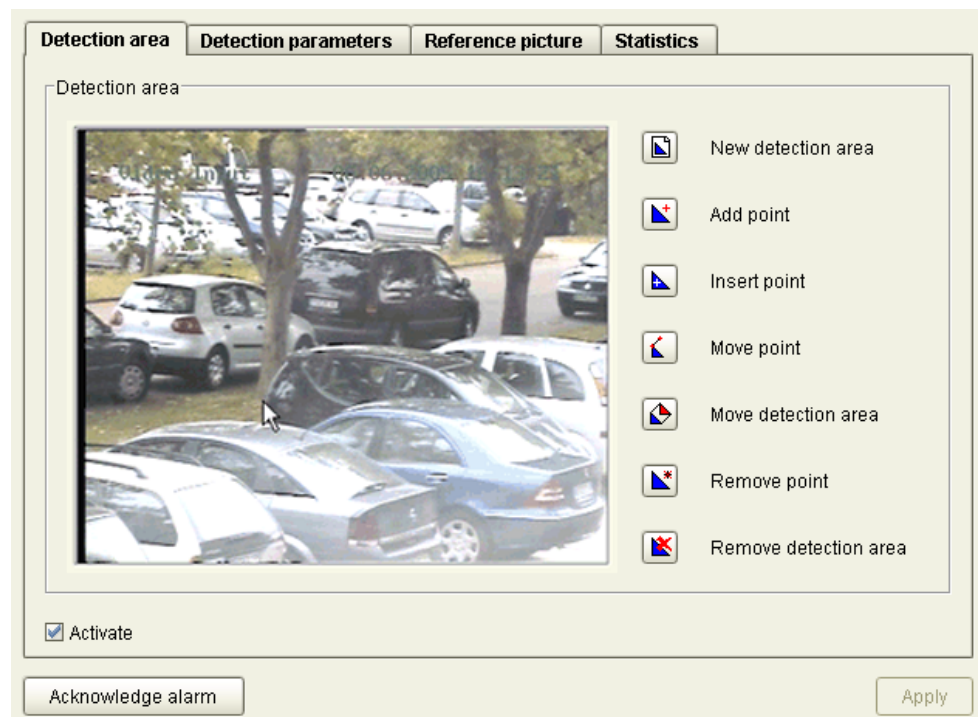
→ The alarm has been acknowledged.

16.7   Configuring a reference image for tamper detection

CX FDV

The reference frame shows the camera's image before it was moved or covered and serves as comparison in the event of a tamper alarm.

1.   In the tree view, navigate to the node representing the video input of the camera whose reference image you want to configure. See Section: 8.4 Configuring video inputs.

2.   Click the **Tamper detection** node.

3.   Select the **Reference picture** tab.

➔ The live video of the camera will be displayed below the tree structure.

4.   Click on **Replace** if you wish to use the displayed live image as reference image for this camera.

5.   Click **Apply**.

➔ The live image is now saved as reference image.

Fig. 105   "Reference picture" tab

16.8   Configuring statistics for tamper detection

CX FDV

1. In the tree view, navigate to the node **Tamper detection**. See Section: 8.4 Configuring video inputs.
2. Select the **Statistics** tab.
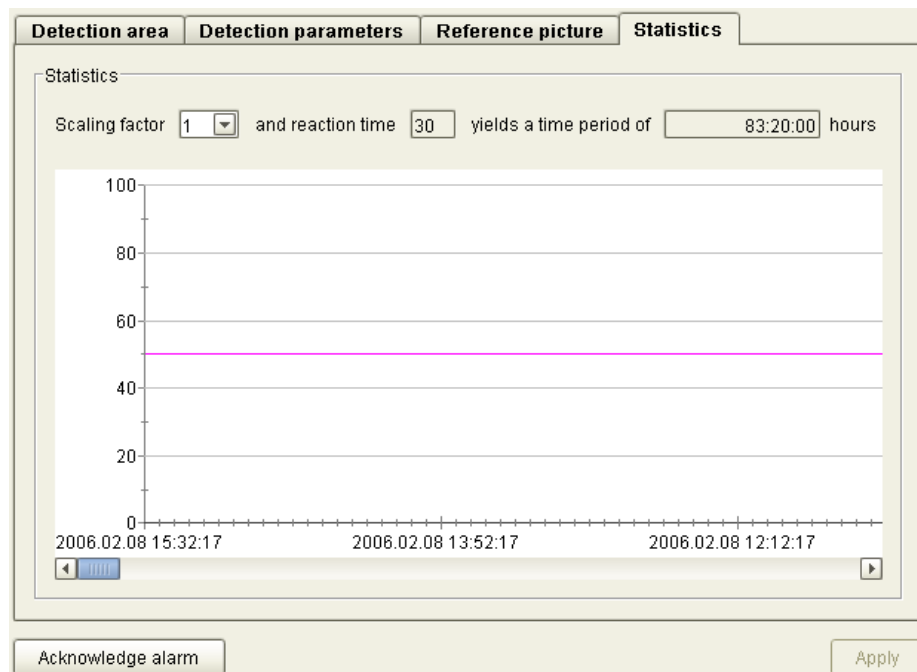
Fig. 106   "Statistics" tab

Scaling factor	The scaling factor is multiplied by the reaction time. This results in the time in seconds after which a measurement will be displayed in the statistics.
Reaction time	Preset in the Detection parameters tab. See Section: 16.4 Defining the detection parameters (tamper detection)
Time period	Time period in hours over which the statistics will be displayed (depending on the scaling factor).

3. Click **Apply**.

17 Configuring image degradation detection

17.1 Symbols for image degradation detection

CX FDV

The symbol for image degradation detection in the tree structure provides the following information:

No colour		Image degradation detection deactivated.
Green checkmark		Image degradation detection activated, no image degradation detected.
Red exclamation mark		Image degradation detected, alarm is triggered.

17.2 Configuring detection parameters and alarm handling

17.2.1 Detection of noise and saturation degradation

Image degradation detection is used to detect deterioration in the quality of the video image. An alarm is triggered when the image is noisy or over-saturated.

1. In the tree view, navigate to the node **Video input**.
2. Select the node **Image degradation detection**.
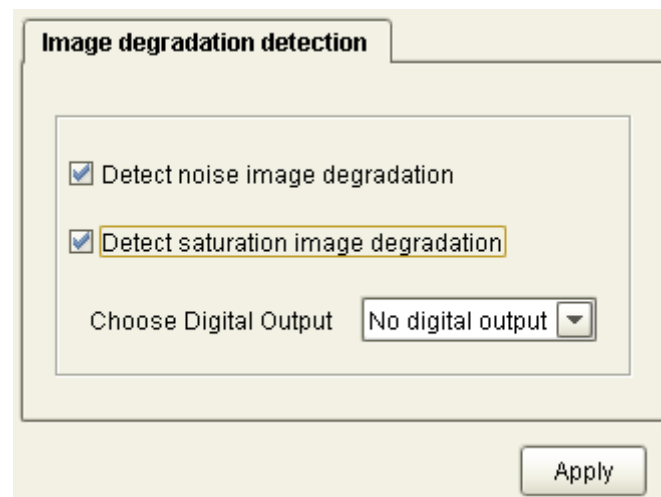
Fig. 107 Image quality – "Image degradation detection"

2. Mark either or both checkboxes **Detect noise image degradation** and **Detect saturation image degradation**.
   → A green checkmark is displayed in the device tree.
3. To define the alarm handling, select a digital output from the list box.
4. Click **Apply**.

18 Rule configuration

CX FDV

The main task of rule configuration consists of the definition and selection of rules. The server requires the rules to perform particular actions after a defined event. A defined event might be a signal change on a digital input for example. The associated action might be to send an alarm and save the event with the pre-event ring buffer recording.

1. Start the SISTORE CX Client application.

2. Select the **Rule configuration** tab .
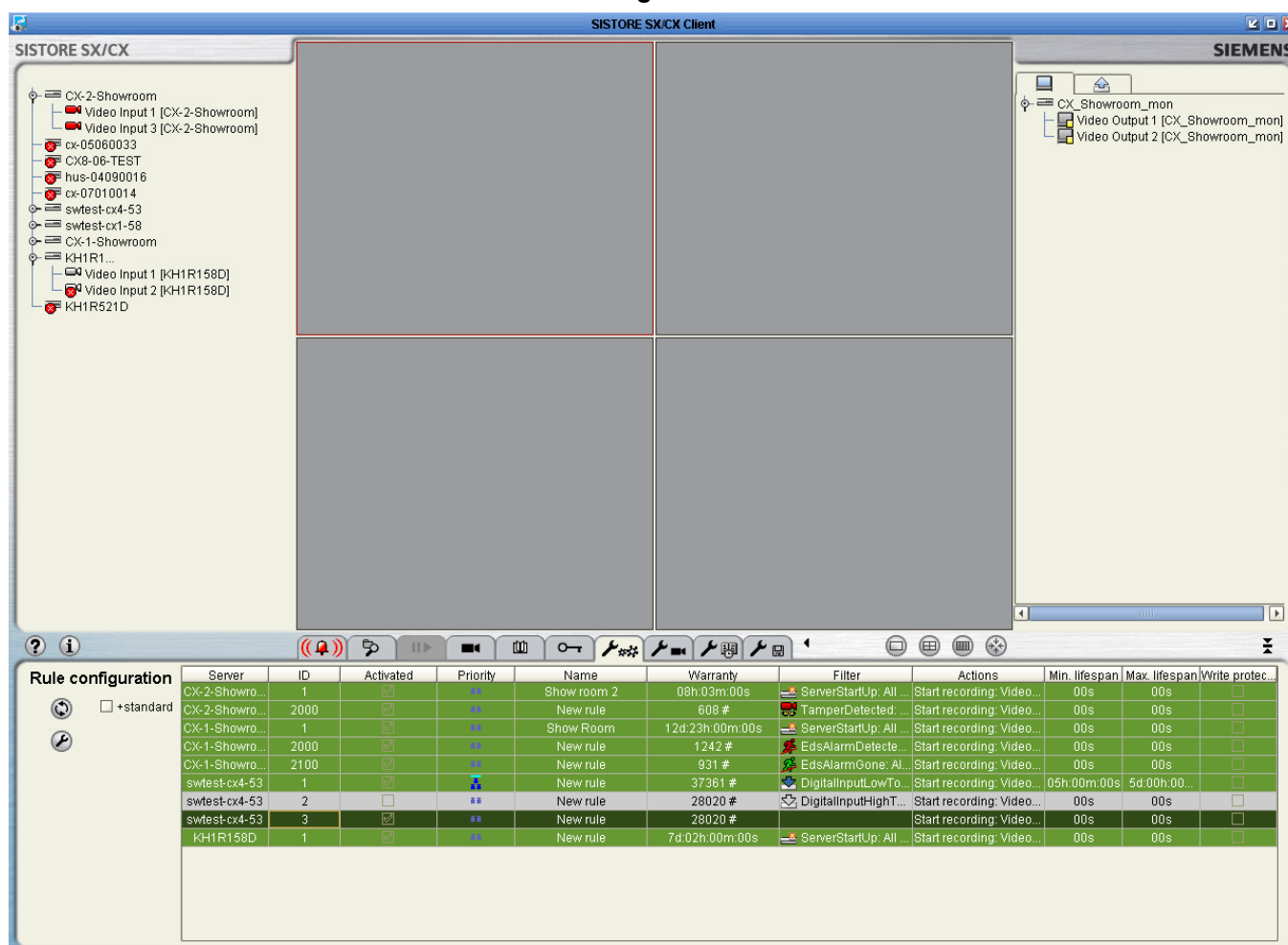
Fig. 108   Rule configuration

---

i
- Rules cannot work across devices without IVM.
- As many as 200 rules per SISTORE device can be configured by the user.

Siemens Building Technologies
Fire Safety & Security Products   03.2009

The following events can trigger rules:
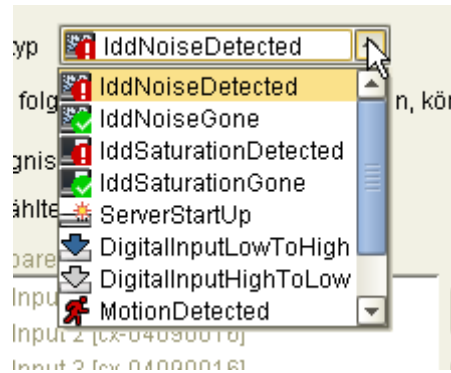
	Applicable to	Event	Explanation
Standard	**Digital inputs**	**DigitalInputLowToHigh**	Change of the digital input level from low to high
		DigitalInputHighToLow	Change of the digital input level from high to low
	Devices (server)	**ServerStartUp**	The device was switched on
	Tampering	**SabotageDetected**	Camera was moved
	Motion detection	**MotionDetected**	Motion detected
	Image degradation detection	**IddNoiseDetected**	Alarm: noisy video image
		IddNoiseGone	Alarm: noisy video image, noise is gone
		IddSaturationDetected	Alarm: saturated video image
		IddSaturationGone	Alarm: saturated video image, saturation is gone
Licence required	**Enhanced motion detection**	**EDSAlarmDetected**	Motion detected
		EDSAlarmGone	Motion is gone
	Detection of removed or left objects	**OdrDetAlarmDetected**	Alarm: left object detected
		OdrDetAlarmGone	Left object is gone
		OdrDetPreAlarmDetected	Pre-alarm: left object
		OdrDetPreAlarmGone	Left object is gone
		OdrRemAlarmDetected	Alarm: object was removed
		OdrRemAlarmGone	Object no longer removed
		OdrRemPreAlarmDetected	Pre-alarm: object was removed
		OdrRemPreAlarmGone	Object no longer removed

18.1 Rule configuration with IVM integration

CX FDV

In an integrated system, the SISTORE device can be controlled via IVM. IVM is a management system for controlling monitoring systems based on various devices.
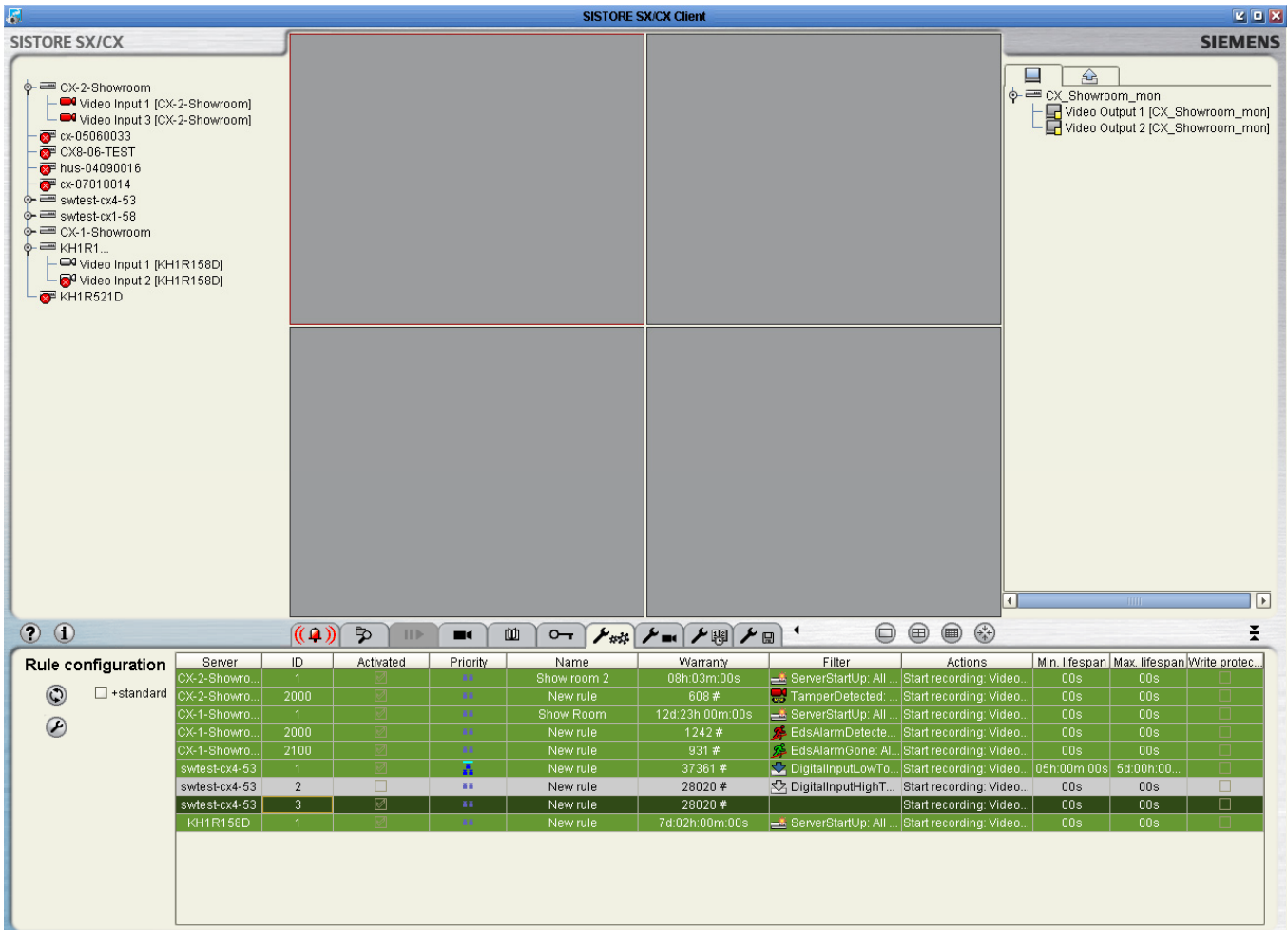
The IVM server sends a command to the SISTORE that determines which SISTORE input is to be recorded for an alarm. The IVM server takes over the entire management of the SISTORE channels. The server determines which video matrix output or SISTORE input the alarm camera connects to.

This ensures optimal use of the SISTORE device resources.

18.2   Rule information

CX FDV

1. Start the SISTORE CX Client application. See Section: 3.15 Starting the software.

2. Open the rule configuration using the [button icon] button.

    ➔ After the rule configurations are displayed, various data for the rules can be read from the list.

Fig. 109   Rules list

Information in the rules list

Rule colour	The rule colour is used to indicate the status of the rule: Green: The rule is active Blue: The rule of an IP camera is active (without guaranteed values) Blue-grey: The encoder settings for live video have priority. The rule is active (without guaranteed values) Yellow: The rule is active (without guaranteed values) grey: The rule is inactive Red: The rule is inactive due to an error
Server	Name of the SISTORE server
ID	Unique rule identifier
Activated	Indicates whether the rule should be active
Priority	The priority is used to resolve conflicts in recording and storage
Name	Name of the rule
Warranty	Guarantees time or number of guaranteed messages

Filter (events)	Event	Explanation
	DigitalInputLowToHigh	Change of the digital input level from low to high
	DigitalInputHighToLow	Change of the digital input level from high to low
	ServerStartUp	The device was switched on
	SabotageDetected	Camera was moved
	MotionDetected	Motion detected
	MotionGone	Motion is gone
	IddNoiseDetected	Alarm: noisy video image
	IddNoiseGone	Alarm: noisy video image, noise is gone
	IddSaturationDetected	Alarm: saturated video image
	IddSaturationGone	Alarm: saturated video image, saturation is gone
	EDSAlarmDetected	Motion detected
	EDSAlarmGone	Motion is gone
	OdrDetAlarmDetected	Alarm: left object detected
	OdrDetAlarmGone	Left object is gone
	OdrDetPreAlarmDetected	Pre-alarm: left object
	OdrDetPreAlarmGone	Left object is gone
	OdrRemAlarmDetected	Alarm: object was removed
	OdrRemAlarmGone	Object no longer removed
	OdrRemPreAlarmDetected	Pre-alarm: object was removed
	OdrRemPreAlarmGone	Object no longer removed

Actions	Actions to be performed when the event occurs. If the action field of a defined rule is left-clicked, all the associated actions will be shown.
Min. lifespan	This indicates the time before a recording for this rule can be overwritten.
Max. lifespan	This indicates the time after which a recording for this rule must be deleted.
Write protection	If this parameter is activated, write-protection is applied to recordings when they are saved.

Further information on the individual rule parameters is found in the following sections.

18.3 Adding a rule

CX FDV

Rule configurations are added using a wizard to guide you through the individual parameter steps. After an entry is made, the wizard offers the option of going to the next or previous dialog box.

1. Start the SISTORE CX Client application. See Section: 3.15 Starting the software.

2. Open the rule configuration. This can be done by clicking the ![wrench icon] button in the toolbar over the working area.

3. Click the button ![button icon] at the left of the rules table.

4. Select the menu item **Add**.

   → The following dialog box opens:

   ℹ️ This dialog will not appear if only one SISTORE server is available; the wizard will start with the next dialog (see Fig. 111) instead.

Fig. 110   "Add Rule - Server selection" dialog box

5. Select the SISTORE server on which you want to configure rules from the drop-down list box.

6. Click **Next**.

➔ The following dialog box opens:

Fig. 111   "Add Rule – General rule parameters" dialog box

The following entries can be made here:

Rule name	**A text description of the rule. The rule name should be unique. It can be between one and 250 characters long.**	
Rule type	The rule type indicates how recordings are to be made and how the recording guarantees are defined. There are the following rule types:	
	Indefinite recording	The recordings run in continuous mode (without interruption) and the oldest part of the recording is overwritten. For the recording guarantees, the time that is guaranteed to be kept on the recording is specified.
	Event-oriented, fixed	The recordings are triggered by events and have a defined follow-up time (post-event). Thus each saved recording has a uniform, fixed length. Thus the recording guarantee is specified by the number of events that are guaranteed to be saved.
	Event-oriented, variable	The recordings are triggered by events but have no predefined post-event recording time. Instead, the follow-up time is specified by the triggering messages. The recording guarantee is specified as total recording time for events of this rule.
Rule should be active	A rule can be set to "active" or "inactive". If the rule is inactive, then there is no check of the recording guarantees when it is created or changed.	
Button **Cancel**	Cancels the rule configuration. No entries will be saved.	
Button **Back**	Continues to the previous dialog box for the wizard.	
Button **Next**	Continues to the next dialog box for the wizard.	
Button **Details**	Definition of additional parameters.	

7.   If the **Details...** button is clicked, the following dialog box appears:

Fig. 112   "Add Rule – General rule parameters" dialog box

The following entries can be made here:

Priority	The priority is used to resolve conflicts in recording and storage. There are the following priority levels:	
	Low	Saved recordings for this rule are deleted first if recordings use more storage than the guaranteed amounts.
	Normal	Saved recordings for this rule are deleted if recordings use more storage than the guaranteed amounts and there are no more low priority recordings to delete.
	High	Saved recordings for this rule are deleted if recordings use more storage than the guaranteed amounts and there are no more low or normal priority recordings to delete.
	High, low execution priority	Saved recordings for this rule are deleted if recordings use more storage than the guaranteed amounts and there are no more low or normal priority recordings to delete. These recordings have a lower recording priority. The recording with the highest execution priority determines the recording parameters.
Write-protection	If this parameter is activated, write-protection is applied to recordings when they are saved. Caution: As soon as the guarantee quantity is exceeded and all events are write-protected, no new events can be saved.	
Minimum lifespan	This indicates the time before a recording for this rule can be deleted. Please note that the minimum lifespan cannot exceed the guarantee time.	
Maximum lifespan	This indicates the time after which a recording for this rule must be deleted.	

8. Click **Next**.

➔ The previous dialog box will be displayed again (see Fig. 111).

9. Click **Next**.

191

→ The following dialog box opens:
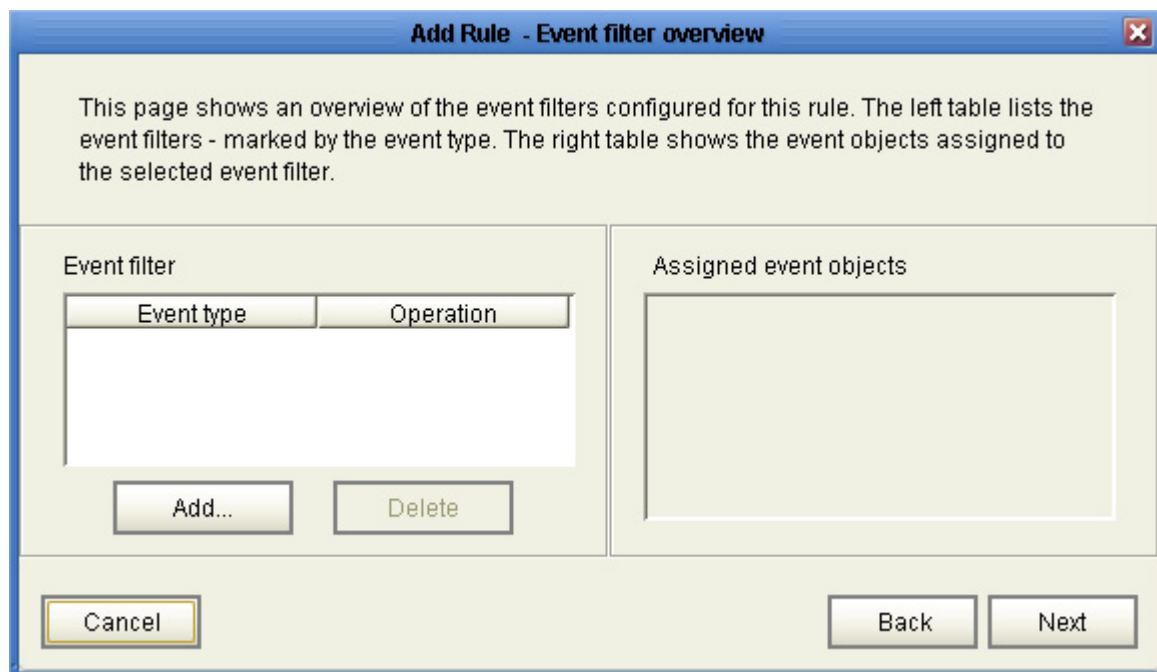
Fig. 113 "Add Rule – Overview of event filters" dialog box

→ This dialog box provides an overview of the event filters configured for the rule. This list is empty when a rule is first created, i.e. no event filters are assigned.

10. To assign an event filter to a rule, click on **Add**.

→ The following dialog box opens:
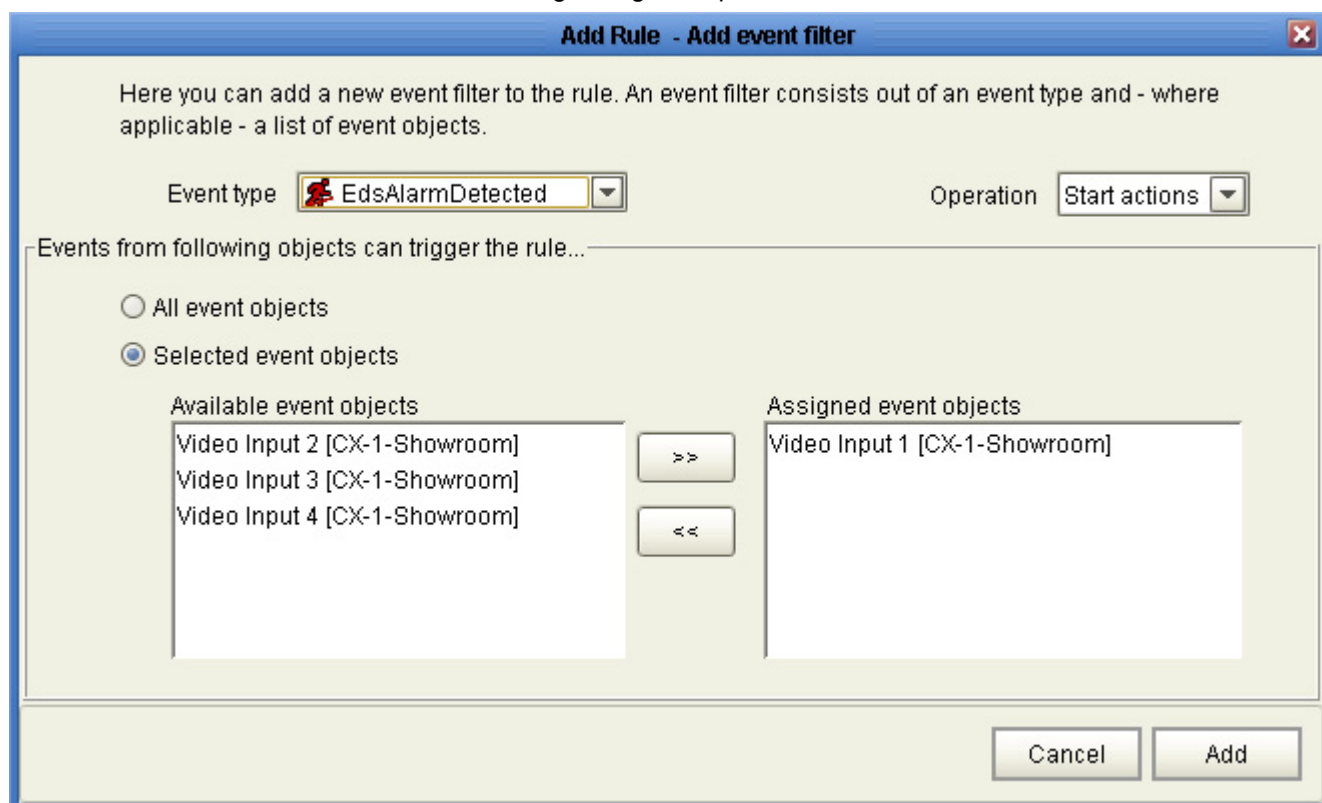
Fig. 114   "Add Rule – Add event filter" dialog box

11. Select the event type you wish to assign to the rule from the **Event type** list box.

12. Depending on the event type, you can determine whether events of this type from any object or only a selected number of objects can trigger the rule.

13. Select an operation from the **Operation** list box. The operation determines whether an action is to be started or stopped.

14. Select the corresponding option to determine whether **all event objects** or only **selected event objects** should trigger the rule.

15. If the rule shall only be triggered by selected event objects, add these to the **Assigned event objects** list. Use **<STRG>** and **<SHIFT>** to make multiple selections.

16. Click **Add**.

→ The previous dialog box will be displayed again (see Fig. 113).

→ The assigned event filters are listed in the **Event filter** table at the left. The table **Assigned event objects** shows all the event objects that were assigned to the selected event filter.

17. Click **Next**.

→ The following dialog box opens:

Fig. 115   "Add Rule – Add recording definition" dialog box

→ In this dialog box, you can define the settings for the video sequences to be recorded by a triggered rule.

| **i** | If a remote video source is selected as the video input when configuring a rule, then it is not possible to select the frame rate, resolution or quality. |

Video input	Only video inputs for which there are no recording definitions in the rule can be set here.
Post-event recording time	The follow-up time can be defined per camera and corresponds to the longest post-event camera recording for this rule. The minimum follow-up time is 5 seconds and the maximum is 30 days.
Use ring buffer	Checkbox marked: The rule runs in the pre-event recording. The corresponding input records continuously. After a defined period, the oldest parts of the recording are deleted. The pre-event recording (ring buffer) is handled in the camera configuration. See Section: 8.4.6 Pre-event parameters. The pre-event parameters thus vary for each input and not for each rule!
Frame rate	The number of images per second that are to be recorded.
Resolution	The format to be used for recorded video sequences. The following formats are supported: QCIF, CIF, 2CIF, DCIF or 4CIF. See Section: 3.1 Operating modes and performance characteristics.
Quality	The higher the image quality, the higher the storage required for a recording. See Section: 24.4 SISTORE CX network utilization and recording times. "Standard" (default) image quality is recommended.

18.   Click **Add**.

➜ The following dialog box opens:
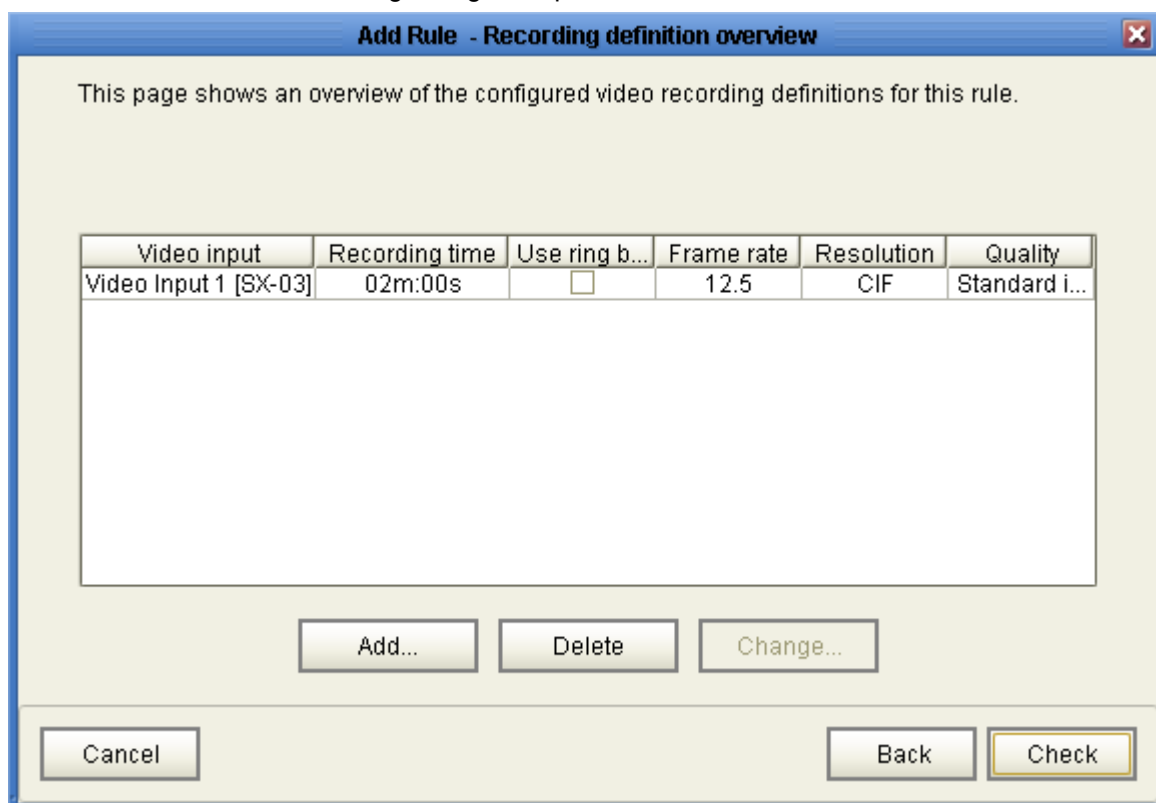
Fig. 116   "Add Rule – Overview of recording definitions" dialog box

➜ In this dialog you can check once more the recording definitions you have made.

19. If you want to add further recording definitions, click on **Add**.

➜ The **Add Rule - Add recording definition** dialog appears again. You can add several recording definitions (one recording per video input).

20. To change a recording definition, select it and click on **Change**.

➜ The **Add Rule - Add recording definition** dialog appears again.

21. To delete a recording definition, select it and click on **Delete**.

> ⚠ If a remote video source is selected as the video input when configuring a rule, then it is not possible to define any guaranteed storage values. The rule configuration is completed at this point.

22. Click on **Check**.

→ The following dialog box opens:
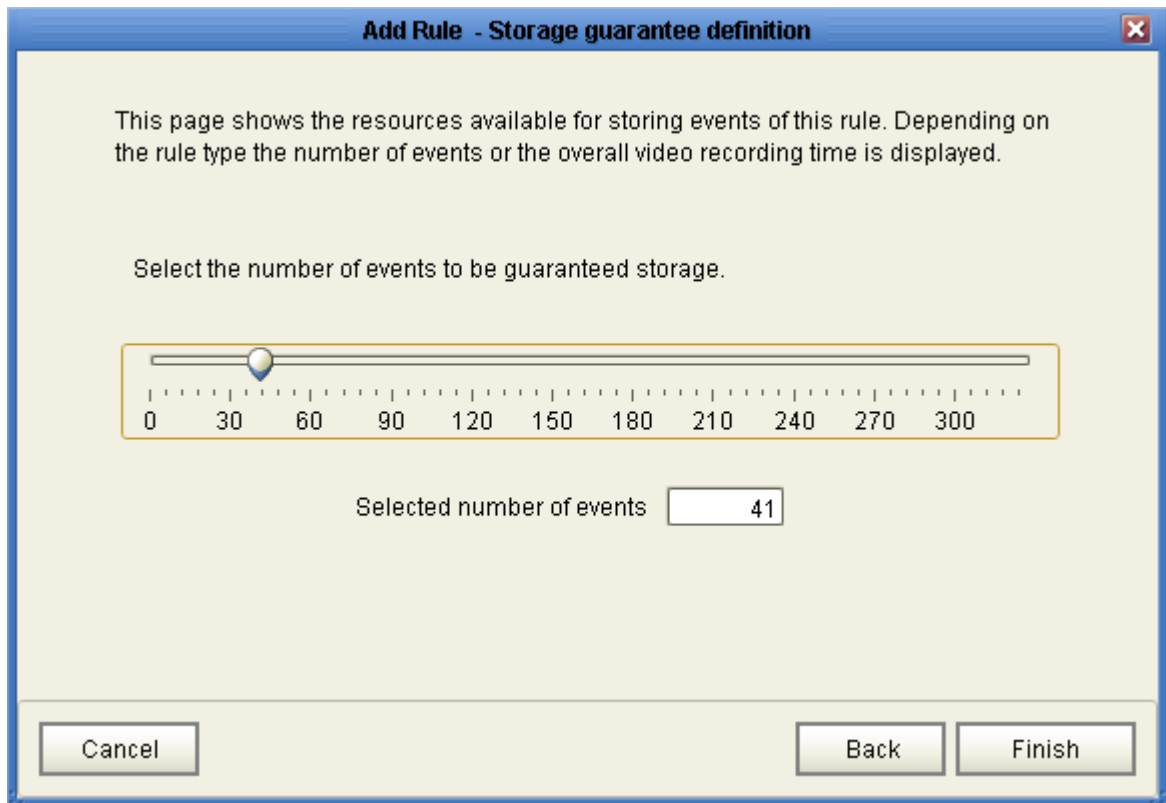
Fig. 117   "Add Rule – Storage guarantee definition" dialog box

→ The available storage resources will be checked. Depending on the rule type, the available storage space will be displayed as a number of events that can be saved or as total recording time. Here you can define the amount of resources to be allocated to this rule (up to the maximum value).

23. Click on **Finish**.

→ The current rule configuration is completed and will be saved.

18.4   Deleting a rule

CX FDV

1. Start the SISTORE CX Client application. See Section: 3.15 Starting the software.

2. Open the rule configuration. This can be done by clicking the 🔧 button in the toolbar over the working area.

3. Select a rule in the working area. Use the **CTRL** and **SHIFT** keys for multiple selections.

4. Choose **Delete** from the **context menu** (right mouse-click).

Fig. 118   Deleting a rule configuration

5. Answer "Yes" in the subsequent confirmation box.

18.5   Changing existing rules

CX FDV

1. Start the SISTORE CX Client application. See Section: 3.15 Starting the software.

2. Open the rule configuration. This can be done by clicking the 🔧 button in the toolbar over the working area.

3. Select a rule in the working area.

4. Choose **Change** from the **context menu** (right mouse-click) or double-click the corresponding rule.

➜ The following dialog box opens:
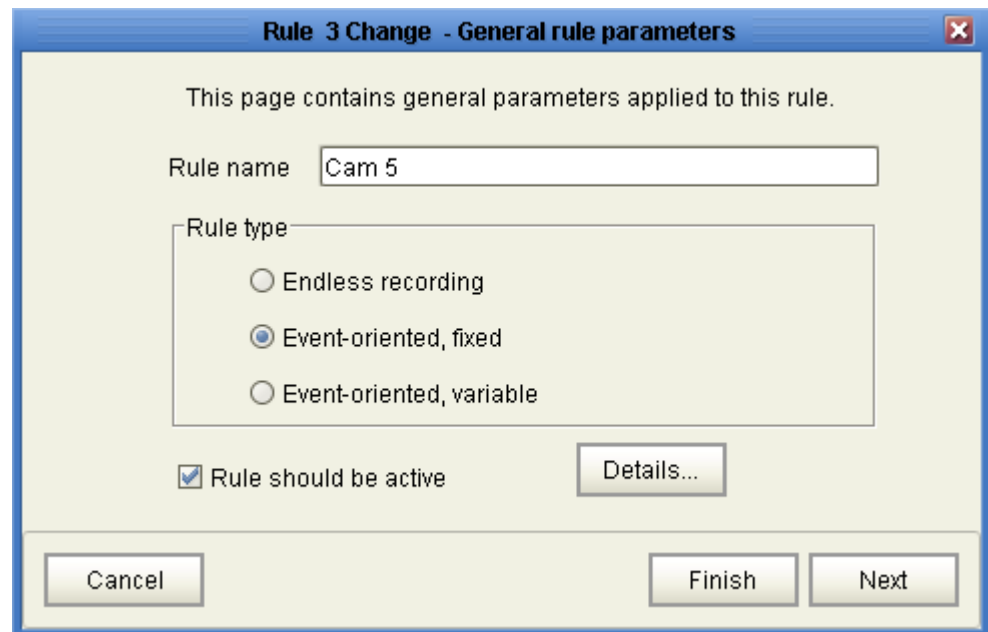
Fig. 119   "Change Rule – General rule parameters" dialog box

5.   Make the desired changes. The individual rule parameters and their configuration options are described in detail in Section: 18.3 Adding a rule.

18.6   Triggering rules

CX FDV

Triggering a rule allows you to start a rule manually.

Prerequisite:

The rule is active.

1.   Start the SISTORE CX Client application. See Section: 3.15 Starting the software.

2.   Open the rule configuration. This can be done by clicking the [button icon] button in the toolbar over the working area.

3.   Select a rule in the working area. Use the **CTRL** and **SHIFT** keys for multiple selections.

4.   Choose **Trigger** from the **context menu** (right mouse-click).
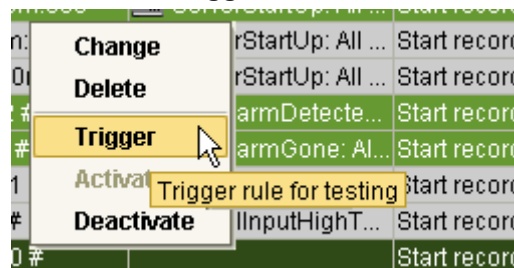
18.7   Stop recordings for a triggered rule

CX FDV

There is no direct command for stopping a recording from an active rule that has been triggered. To stop the recording, the relevant rule must be deactivated and subsequently reactivated. See Section: 18.8 Activating / deactivating rules.

⚠	**IMPORTANT**	Make sure that rules stopped this way are reactivated in each case. If it is not activated, a rule cannot be triggered by automation (such as trigger events).

18.8   Activating / deactivating rules

CX FDV

The rule configuration offers the option to activate and deactivate rules. This makes sense if a rule is not needed for a certain period but should not be deleted. The rule can be set to "inactive" so that it is not affected by triggering events.

Deactivating a rule

1.   Start the SISTORE CX Client application. See Section: 3.15 Starting the software.

2.   Open the rule configuration. This can be done by clicking the [button icon] button in the toolbar over the working area.

3.   Select a rule in the working area. Use the **CTRL** and **SHIFT** keys for multiple selections.

4.   Choose **Deactivate** from the **context menu** (right mouse-click).

➔ The rule is then displayed with a grey background.

➔ If a rule is deactivated, the storage space originally reserved for this rule is released.

Fig. 120   Deactivated rules

Activating a rule

1. Start the SISTORE CX Client application. See Section: 3.15 Starting the software.

2. Open the rule configuration. This can be done by clicking the ![icon] button in the toolbar over the working area.

3. Select a rule in the working area. Use the **CTRL** and **SHIFT** keys for multiple selections.

4. Choose **Activate** from the **context menu** (right mouse-click).

   → The rule is then displayed with a green background.

   → If a rule is reactivated after deactivation, it may be displayed with a yellow background. This means that the storage quantity (space or number) can no longer be guaranteed.

18.9 Rules and internal events

CX FDV

Rule selection works according to the **best match principle**, i.e. the attempt is made to find rules that best fit an event that has occurred. The rule selection procedure works like this:

First a check is made to see if there are rules that fit the event exactly. An event fits a rule (or more precisely an assigned event filter) precisely if the type of the filter and the event type are the same and additionally either both the filter and the event have no assigned objects or the event object of the event is also assigned to the filter.

If there are rules that fit the event exactly, only these will be run. If there are no rules that fit exactly, a search is made for all rules that have a filter of the same type as the event but have no event objects assigned. If rules like this are found, they will be run.

● Example:

There are two rules defined:

Rule 1 with an event filter of the type "input level changes from low to high" on input 1 and the action of starting a recording on video input 1 at 25 ips.

Rule 2 with an event filter of the type "input level changes from low to high" without an assigned event object and the action of starting recording on all video inputs at 2 ips.

If an event of the relevant type occurs on the digital input 1, only rule 1 is triggered. If an event of the same type occurs on any other digital input, only rule 2 is triggered.

19 Configuring export of video sequences

Export of video sequences

When the export of video sequences is configured, the recorded sequences saved on the SISTORE unit will be exported to another data medium. Recordings that were saved to an external data medium can be replayed at any time with the SISTORE CX Player, independent of the SISTORE unit. See Section 19.4 Running export of video sequences.

Task

A task is an action that defines which recordings will be exported. See Section 19.2 Creating a task. A task is defined by the following properties:

Properties	Definition
Start and duration	Start and duration define the time period for which recordings are to be exported.
Video input	By selecting video inputs you can define that only the recordings for specific video inputs will be exported. See Section 19.3.1 Assigning video inputs.
Filter	By assigning filters you can define that specific events or rules are to be applied. See Section 19.3.2 Assigning filters. Using rules it is for instance also possible to export recordings triggered by IVM only.

Example – Tasks and start of export of video sequences
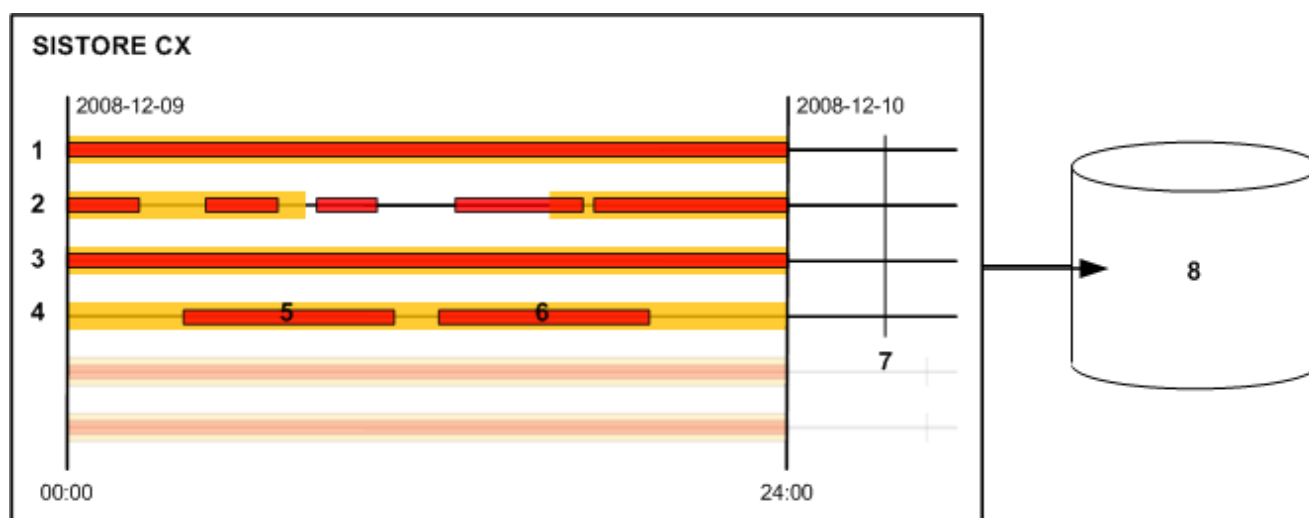
Fig. 121 Example of tasks and start of export of video sequences

▮ (red)	Recording	
▬ (orange)	Time period of the task	
1, 3	Video inputs1 ad 3: Long-time recording	
2	Video input 2: Recordings that are started within the defined time period will be exported.	
4	Video input 4: Event-oriented recording, motion detection, and enhanced motion detection	
	5	Recording of an enhanced motion detection
	6	Recording of a tamper detection
7	Start of the export of video sequences. Export of all tasks on the following day.	
8	Data medium	

19.1 Directory for exported video data

CX FDV

> **ℹ NOTE**
> It is not possible to export recordings that were started manually from the SISTORE CX Client.

Prerequisite:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Swap-Out Config application. See Section: 3.15 Starting the software.

2. In the tree view, navigate to the node **Video Swap-Out**.
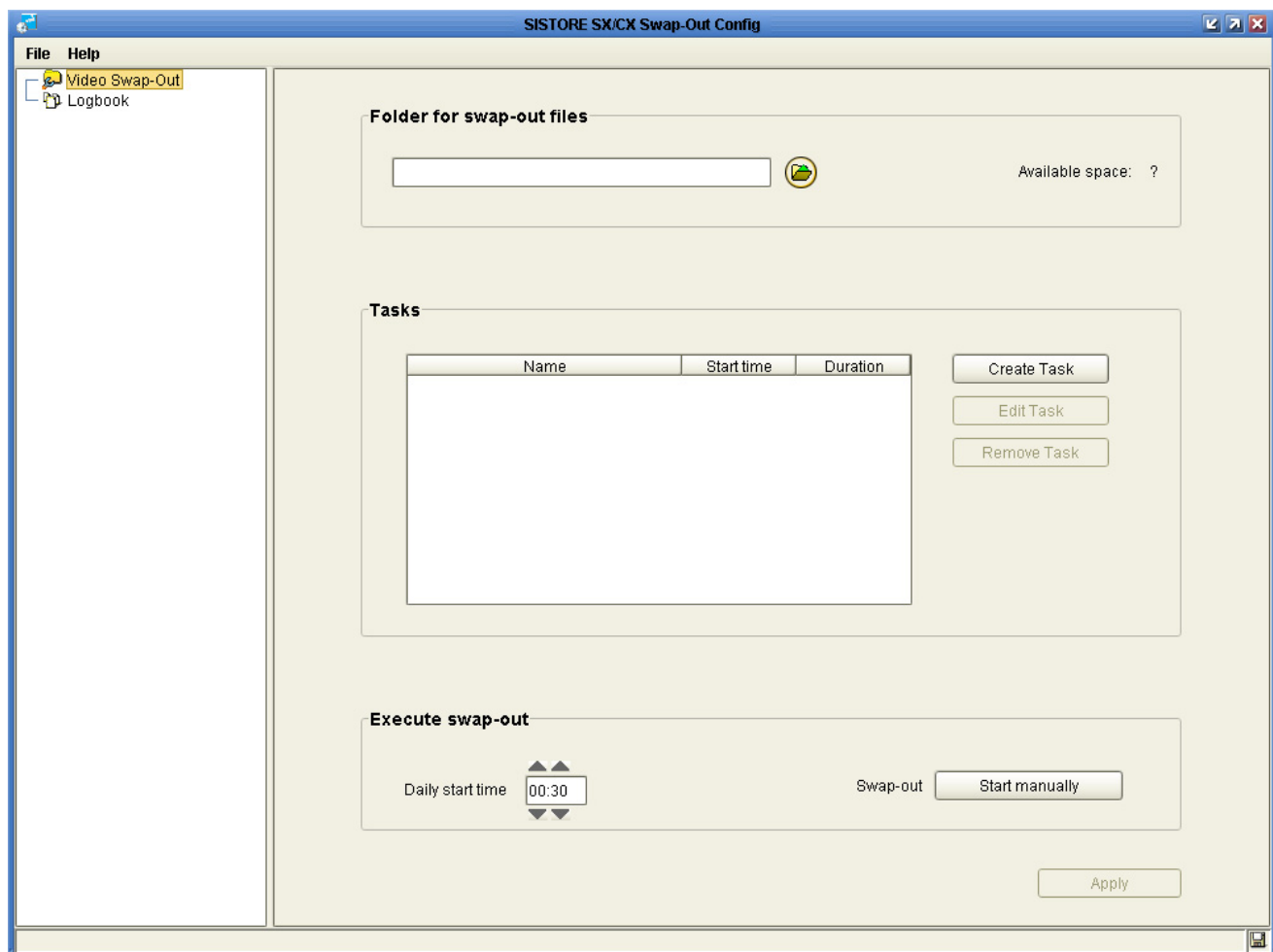
Fig. 122   Video swap-out

3. Click on the folder icon.
4. Select a directory.
5. Click **Apply**.

> **ℹ** If you want to back up the video swap out files on a network drive, you have to configure an AT service account.

AT service account configuration

1. Select **Start** > **Settings** > **Control Panel** in the Windows start menu.
    → The **Control Panel** window will open.
2. Double click on **Scheduled Tasks**.
3. Select the menu sequence **Advanced > AT Service Account**.
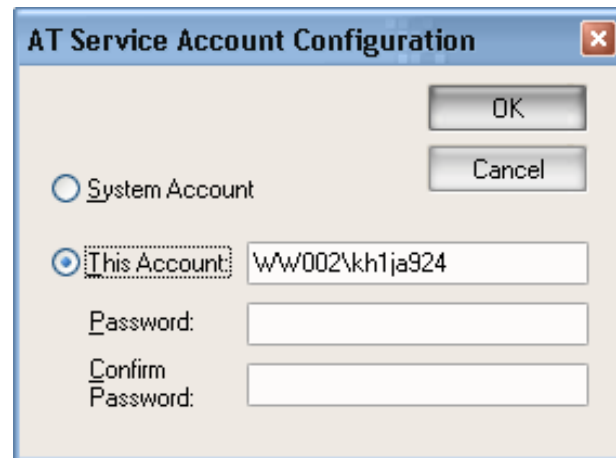
Fig. 123   AT service account configuration

4. Select the option **This Account**.
5. Enter an account with access to the network and the appropriate password.
6. Click **OK**.

19.2   Creating a task

CX FDV

Prerequisite:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

1.   Start the SISTORE Swap-Out Config application. See Section: 3.15 Starting
      the software.
2.   In the tree view, navigate to the node **Video Swap-Out**.
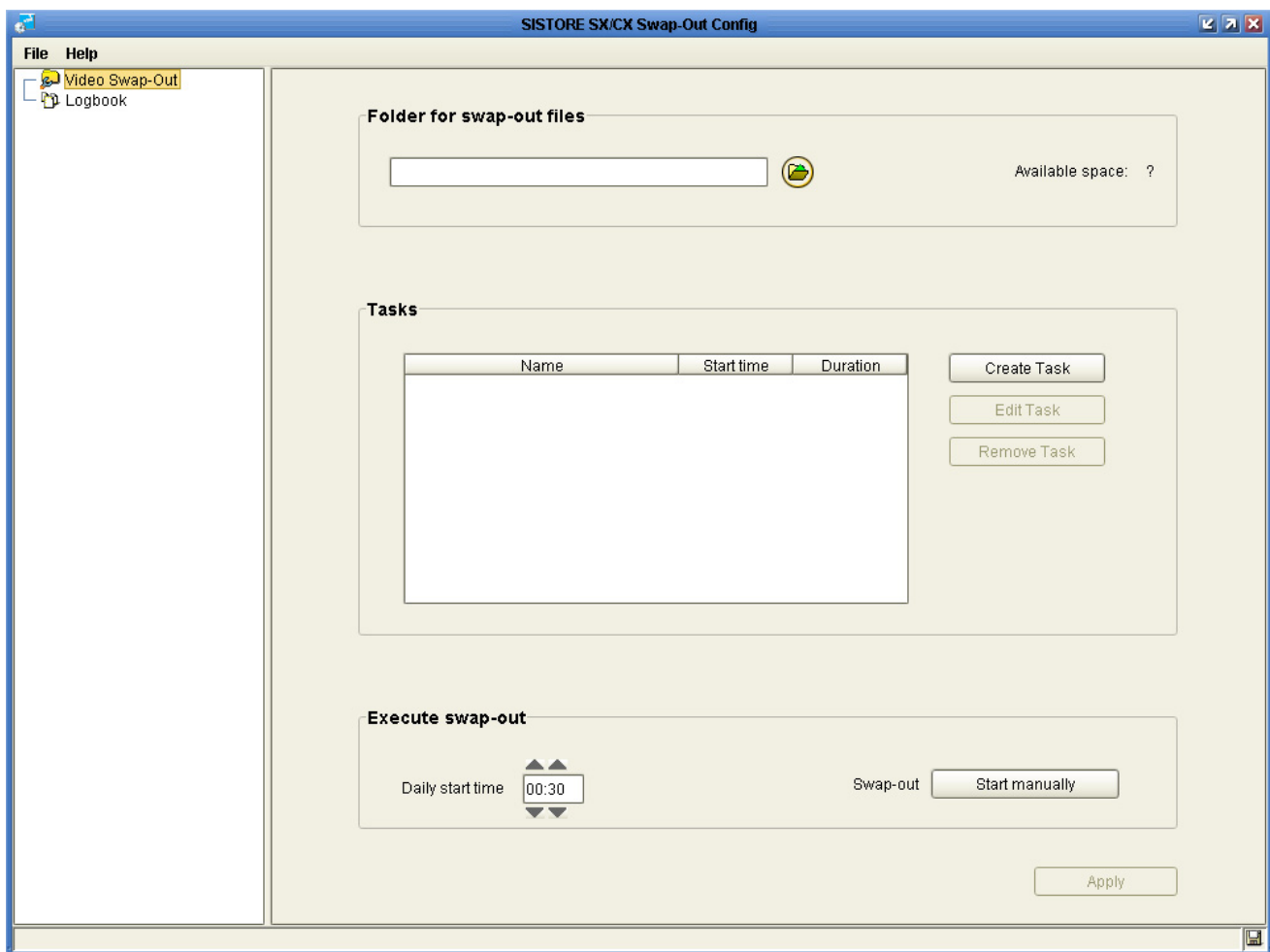
Fig. 124   Configuring export of video sequences

3.   Click on **Create Task**.

➔ The **Create Task** dialog box opens.

Fig. 125   "Create Task" dialog box

4.   Make the following settings in this tab:

Name	Name of the task
Start time	Start and duration define the time period for which recordings are to be exported.
Duration	Sequences will only be exported if the recording started within this time period.

➔ The minimum data for a new task has now been entered.

5.   Click **Apply**.

– OR –

Make further settings in the **Video Inputs** and **Filter** tabs. See
Section: 19.3 Configuring a task .

➔ The task will appear in the device tree.

19.3 Configuring a task

19.3.1 Assigning video inputs

CX FDV

Prerequisite:

A task has been created. See Section: 19.2 Creating a task.

| **i** | **NOTE** |
| | If a video input is displayed in red, this means that it is currently not available. |

1. In the tree view, navigate to a **Task**.
2. Select the **Video inputs** tab.
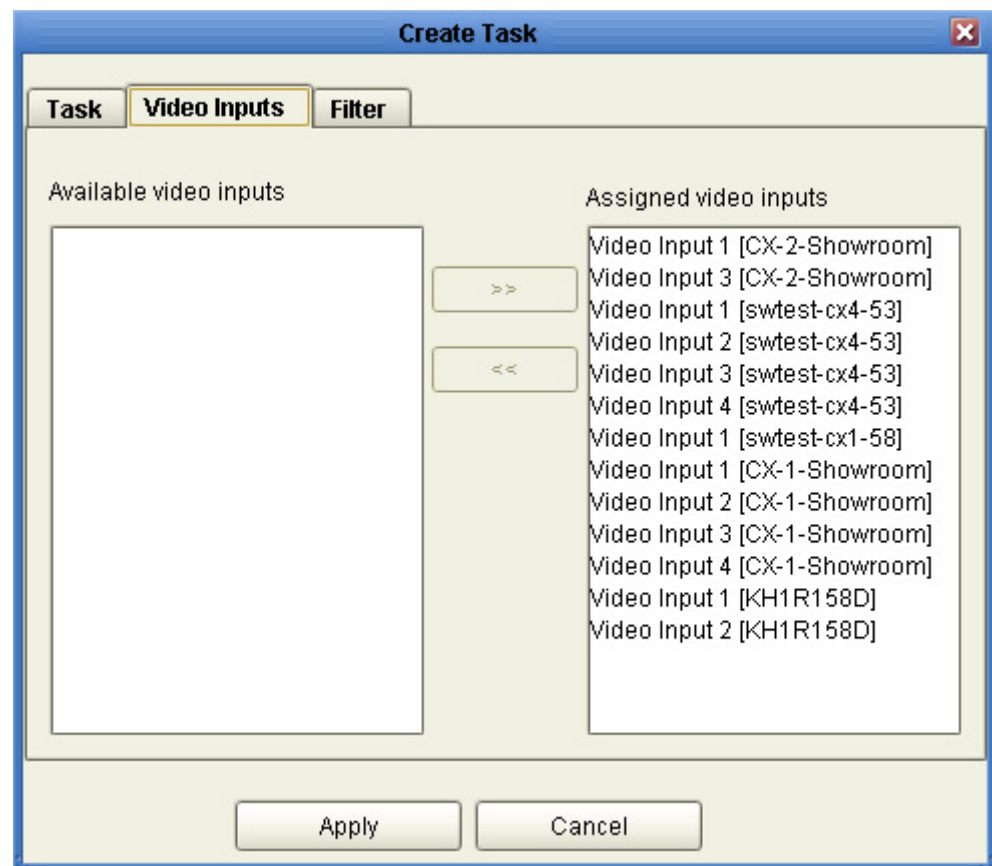
Fig. 126   "Video inputs" tab

| **i** | In the default condition, all video inputs are assigned to a task. |

3. If a video input is not to be assigned to a task, select it in the **Assigned video inputs** list.
4. Click on **<<**.
   → The video input appears in the **Available video inputs** list and is no longer assigned to the task.
5. Click **Apply**.

19.3.2 Assigning filters

CX FDV

Prerequisite:

A task has been created. See Section: 19.2 Creating a task.

1. In the tree view, navigate to a **Task**.
2. Select the **Filter** tab.
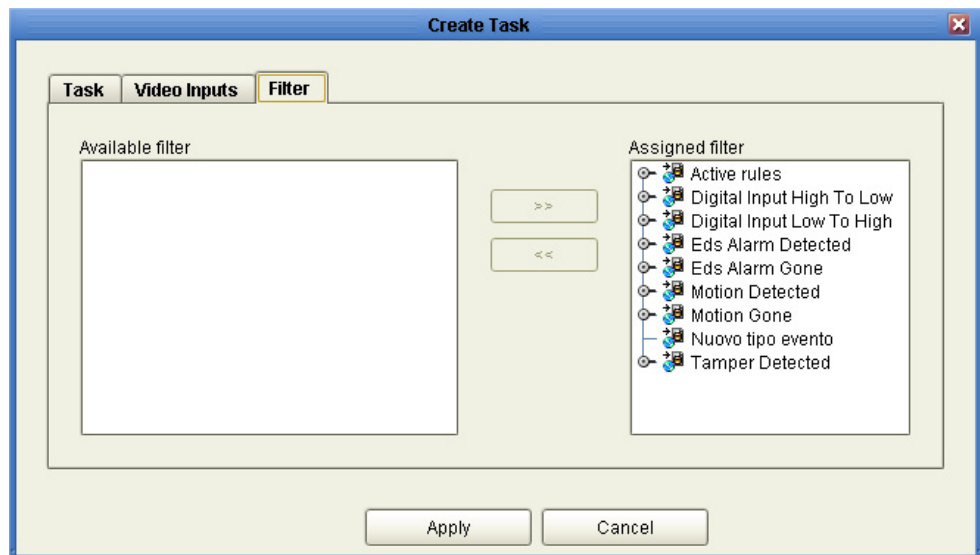
Fig. 127   "Filter" tab

NOTE

The video inputs (see Section 19.3.1 Assigning video inputs) and filters are ANDed.

In order that recordings can be exported, there must be recordings from the selected video inputs with the selected filter being applied.

In the default condition, all filters are assigned to a task.

---

3. If a filter is not to be assigned to a task, select it in the **Assigned filter** list.
4. Click on **<<**.
   ➔ The filter appears in the **Available filter** list and is no longer assigned to the task.
5. Click **Apply**.
   ➔ Active rules are displayed in the node **Active rules**. See Section 18 Rule configuration.

NOTE

Please note that the defined rules also have an effect on the export of video sequences.

19.4 Running export of video sequences

CX FDV

All the tasks triggered the day before are exported.

There are two possible ways to export video data to another data medium:

● Starting an automatic daily export. See Section: 19.4.1 Automatic daily export of video sequences.

– OR –

● Start a one-time manual export of video sequences. See Section: 19.4.2 One-time manual export of video sequences.

Prerequisite:

A task has been created. See Section: 19.2 Creating a task.

> **i** **CPU load during export up to 100 %**
> ● We recommend exporting the video data either to a separate PC or during the night.
> ● Install the SISTORE CX and the PC for exporting the data in a dedicated network segment.

1. In the tree view, navigate to the node **Video Swap-Out**.
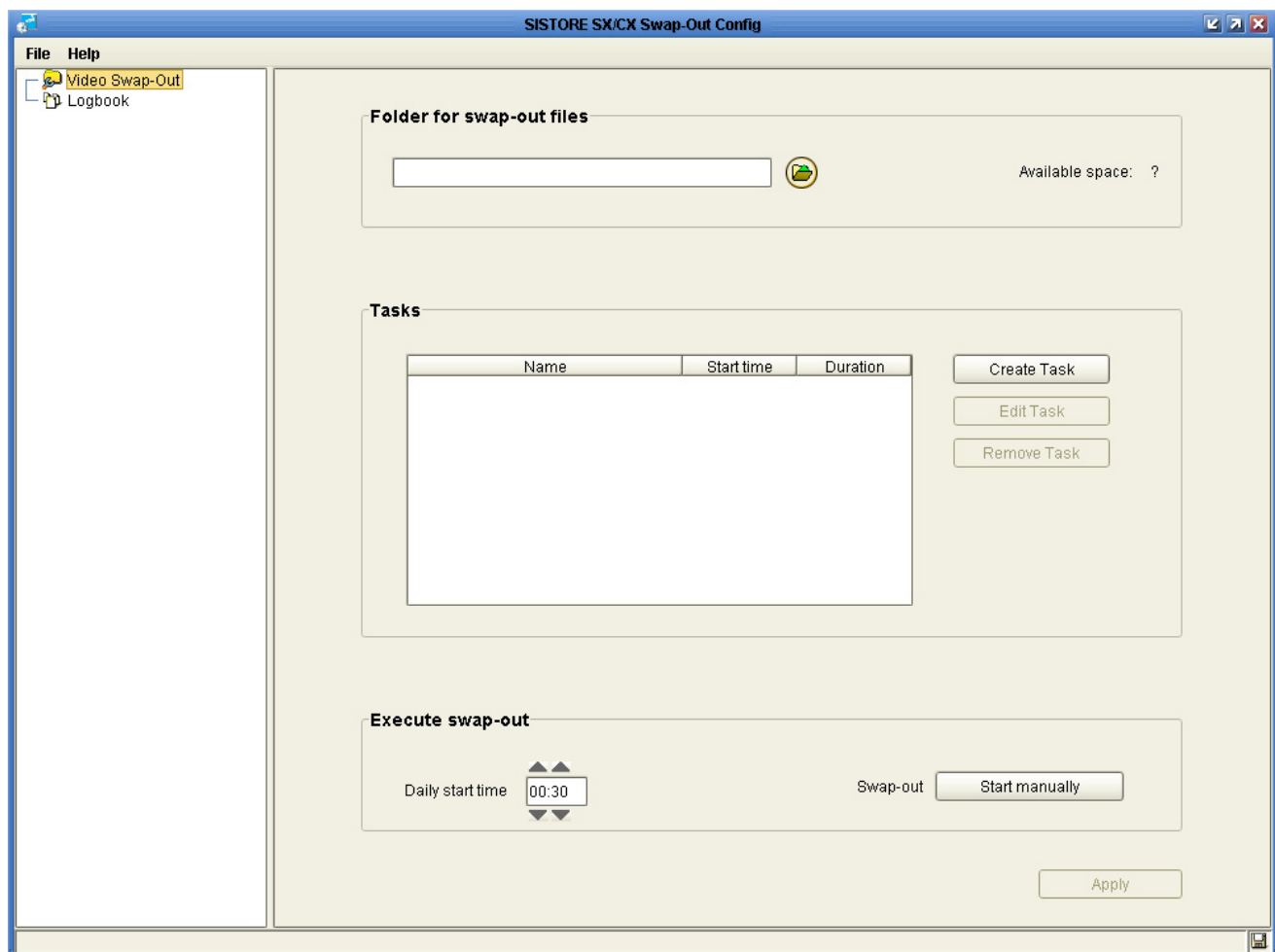
Fig. 128   Video swap-out

19.4.1 Automatic daily export of video sequences

CX FDV

> **i** All the tasks triggered the day before are exported.

1. Enter a time in the **Daily start time** box.
2. Click **Apply**.
3. To display the status of a current swap-out process, rest the mouse pointer on the icon in the status bar for a moment.
   → The following information will be displayed:

   Video Swap-Out is running

   aeble-cx4-24: 4/124
   swtest-cx1-57: 1/40
   swtest-cx4-53: 4/5
   swtest-cx8-55: 5/96
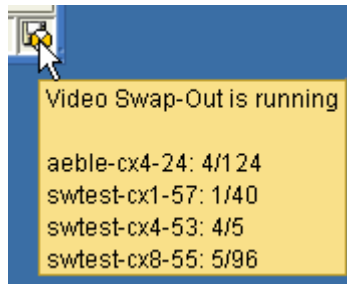
   [Server name]: [active jobs]/[total number of jobs]
   → In the logbook and in the Windows task bar you can see whether the export was successful. See Section: 19.6 Opening the video swap-out logbook and Section: 19.7 Information in the status bar.
   → Failed tasks will be started again when the next export task is performed.

19.4.2 One-time manual export of video sequences

CX FDV

> ℹ️ All the tasks triggered the day before are exported.

1. Click on **Start manually**.

2. To display the status of a current swap-out process, rest the mouse pointer on the icon 🔲 in the status bar for a moment.

   ➜ The following information will be displayed:

   Video Swap-Out is running

   aeble-cx4-24: 4/124
   swtest-cx1-57: 1/40
   swtest-cx4-53: 4/5
   swtest-cx8-55: 5/96
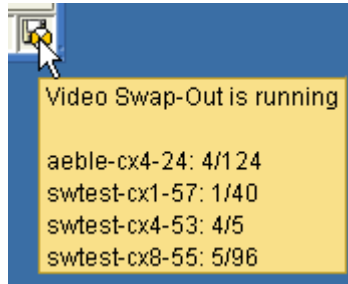
   [Server name]: [active jobs]/[total number of jobs]

   ➜ In the logbook and in the Windows status bar you can see whether the export was successful. See Section: 19.6 Opening the video swap-out logbook and Section: 19.7 Information in the status bar.

   ➜ Failed tasks will be started again when the next export task is performed.

19.5 Examples for exporting video data

19.5.1 Manual export of video sequences

CX FDV

Only the tasks that were triggered the day before are exported.

For a manual export of video sequences to an external storage medium, the start time of the task is selected manually. See Section: 19.4 Running export of video sequences.

19.5.2 Automatic daily export of video sequences

CX FDV

Export all recordings

Based on the task properties in the example shown below, all the recordings made between 00:00 and 24:00 the previous day (2008-12-09) will be exported.

The export of video sequences to any desired data medium is started at 00:30 on the following day (2008-12-10).

Details of the task	
Start time	00:00 hrs
Time period	24 hours
Start of export of video sequences to any desired data medium	
Start time	00:30 hrs
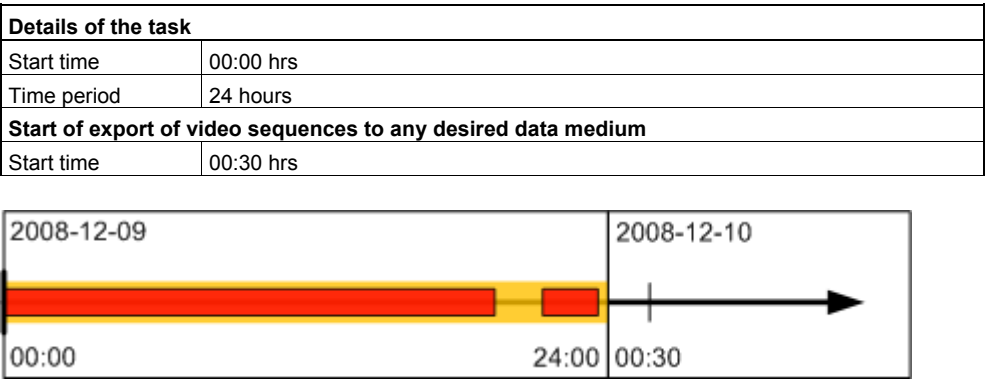
Fig. 129 Recording duration and start of export of video sequences

▮ Recording	
▬ Time period of the task	
ℹ	**NOTE** All the recordings that are started within the defined time period will be exported.
00:30	Start of export of video sequences

Export event-oriented recordings

Task 1: The recordings made the day before (2008-12-09) between 00:00 and 08:00 in which the event "MotionDetected" occurred are prepared to be exported.

Task 2: The recordings made the day before (2008-12-09) between 17:00 and 24:00 in which the event "SabotageDetected" occurred are prepared to be exported.

The export of video sequences for all tasks to any desired data medium will be started at 00:30 on the following day (2008-12-10).

Details of task 1	
Start time	00:00 hrs
Time period	8 hours
Event	MotionDetected
Details of task 2	
Start time	17:00 hrs
Time period	7 hours
Event	SabotageDetected
Start of export of video sequences to any desired data medium	
Start time	00:30 hrs
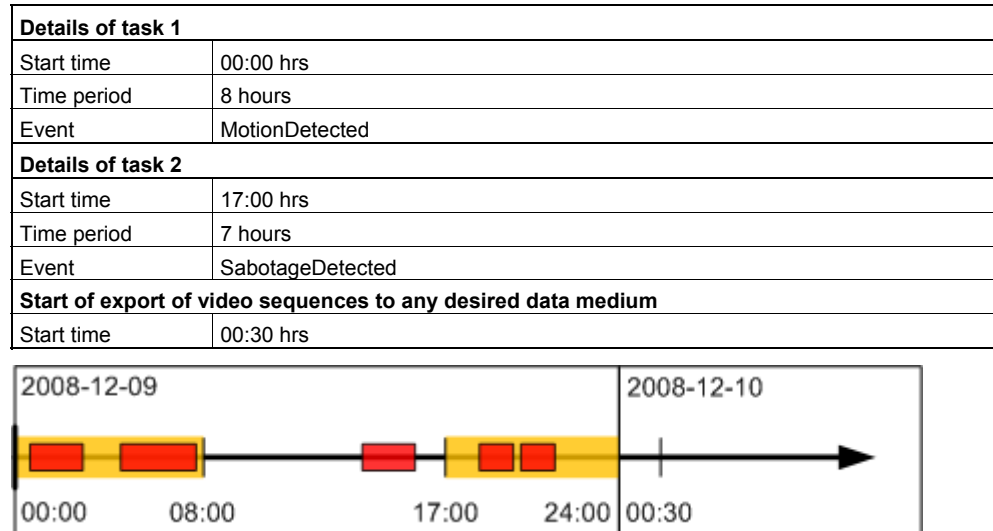
Fig. 130   Event-oriented recording and start of export of video sequences

▮	Recording
▬	Time period of the task
	NOTE All the recordings in which a motion or tampering was detected and which started within the defined time period will be exported.
00:30	Start of export of video sequences

19.6   Opening the video swap-out logbook

CX FDV

The logbook shows the status of export tasks. Failed tasks will be started again when the next export task is performed.

Prerequisite:

A task has been created and executed. See Section: 19.2 Creating a task.
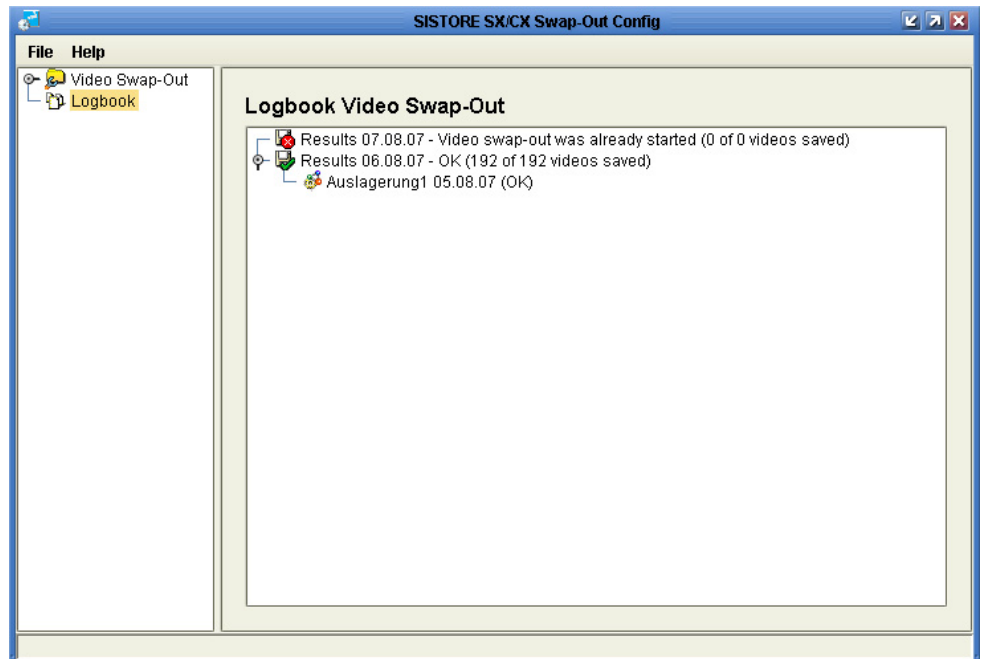
Fig. 131   Video swap-out

i   Logbook entries are deleted after one month.

19.7 Information in the status bar

CX FDV

	No video swap-out task has been started
	Video swap-out in progress
	Last video swap-out was successful
	Error during video swap-out

19.8 Searching and playing videos

CX FDV

Search videos

In the directory you have selected for the exported files, SISTORE CX Swap-Out Config will create the following folders:
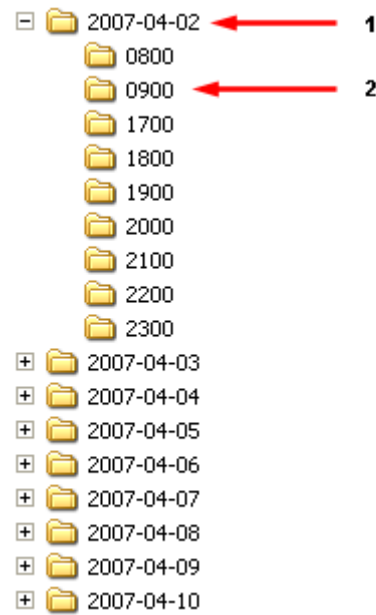
Fig. 132   Folder structure for exported video files

1	Day on which video was recorded
2	Time when video was recorded

The recordings will be saved to the folder(s) for the corresponding hour(s). If the duration of a recording exceeds an hour by less than 5 minutes, the excess time will not be saved to a new folder. See example below:

Recording	Folder
01:54 to 02:04:59	0100
01:54 to 02:05:01	0200

Play videos

1. Start the SISTORE Player. See Section: 3.15 Starting the software.
2. Open a video.

19.9   Ignoring failed tasks

CX FDV

1. In the tree view, navigate to the node **Logbook**.
2. Select a failed task.
3. Right-click on a task.
4. Select **Ignore task**.

20 NAS configuration

CX **FDV**

An NAS (Network Attached Storage) can be used as an external data medium. For this purpose, the NAS has to be configured both with the NAS software Windows 2003 Storage Server and with SISTORE CX Config (see Sections: 20.1 Configuring NAS with Windows 2003 Storage Server and 20.2: Configuring NAS using SISTORE CX Config).

We recommend you to

- assign each SISTORE CX its own partition on the NAS.
- arrange small partitions as RAID 1 and large partitions as RAID 5 or RAID 6.
- connect the NAS in teaming mode via several network links. The switch as well as the network cards in the NAS must be capable of teaming for this.

IMPORTANT	**Data loss during recording** If the data volume transmitted is very large, there is a risk of data being lost. - Make sure that the data volume handled by the recording devices is less than 60 % of the nominal data rate of the NAS. - Make sure that the data volume handled by the recording devices is less than 60 % of the nominal data rate of the CX devices. - Make sure that the data volume handled by the recording devices is less than the internal write/read data rate of the NAS system.

IMPORTANT	**Data loss after a rebuild** - During a rebuild, individual images may be lost.

Examples of NAS server performance
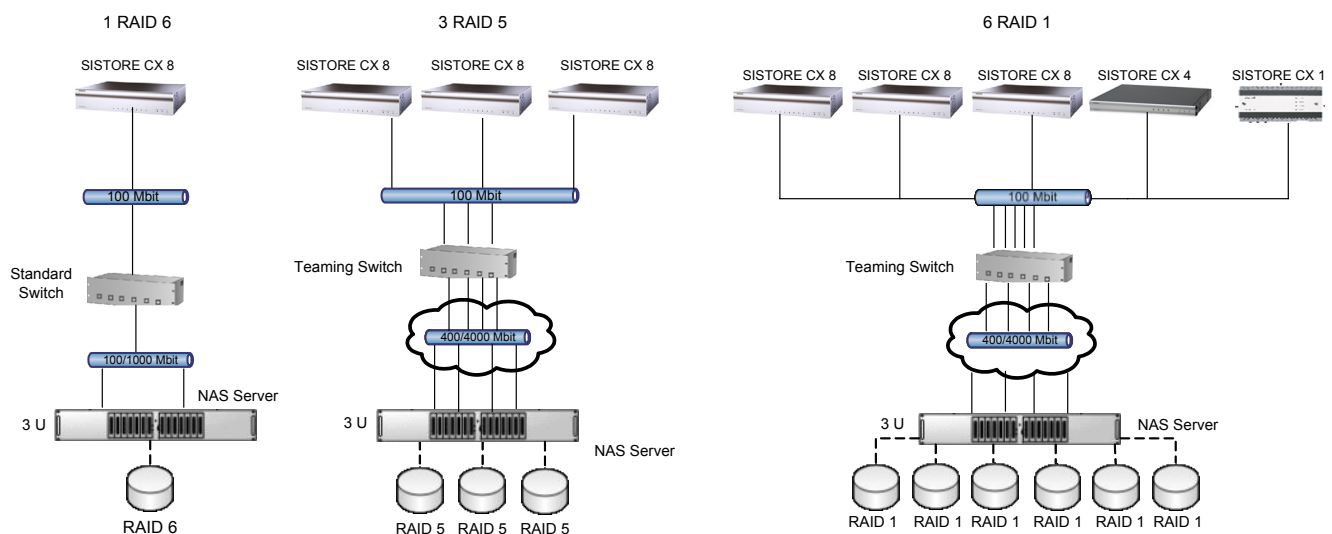
Fig. 133   Examples of NAS server performance

Siemens Building Technologies
Fire Safety & Security Products

	1 x RAID 6	3 x RAID 5	6 x RAID 1	Comment
Switches/ network cards	Standard	Teaming capability	Teaming capability	Using network cards with teaming capability the resulting backbone is as follows: – with a 100 Mbit network: 400 Mbit – with a 1 Gbit network: 4 Gbit
Data security	Very high	High	Medium	–
Network cards on the server	1	4	4	3 x RAID5 and 6 x RAID1: the 4 network cards with teaming capability are combined in 1 entity and the 4 network ports are combined in 1 network port. All frame stores access one IP.
Reliability of the network cards	✕	✓	✓	1 x RAID6: not fail-safe as the frame stores are connected one-to-one to the servers.
Server performance	Medium	High	Very high	1 x RAID 6: 1 x RAID 6 for 1 frame store (max. 1 x CX8) 3 x RAID 5: 3 x RAID 5, physically separated drives (max. 3 x CX8) 6 x RAID 1: 6 x RAID 1, physically separated drives on the server (e.g. 3 x CX8, 1 x CX4, 1 x CX1)

20.1   Configuring NAS with Windows 2003 Storage Server

CX FDV

Prerequisites:

You have admin user rights.

You have a password.

Starting the Windows 2003 Storage Server

1.   Switch the NAS on.

→ The Windows 2003 Storage Server software is started automatically.

2.   Log on to the software:

If no administrator password has been assigned yet, create a password.

– OR –

If an admin password exists already, change it after you have logged on.

i   We advice not to change the password again after this.

Assign computer name

1.   Right-click on the desktop icon **NAS-Server**.
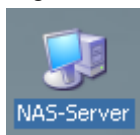
2.   Select **Properties**.

➔ The following dialog box opens.
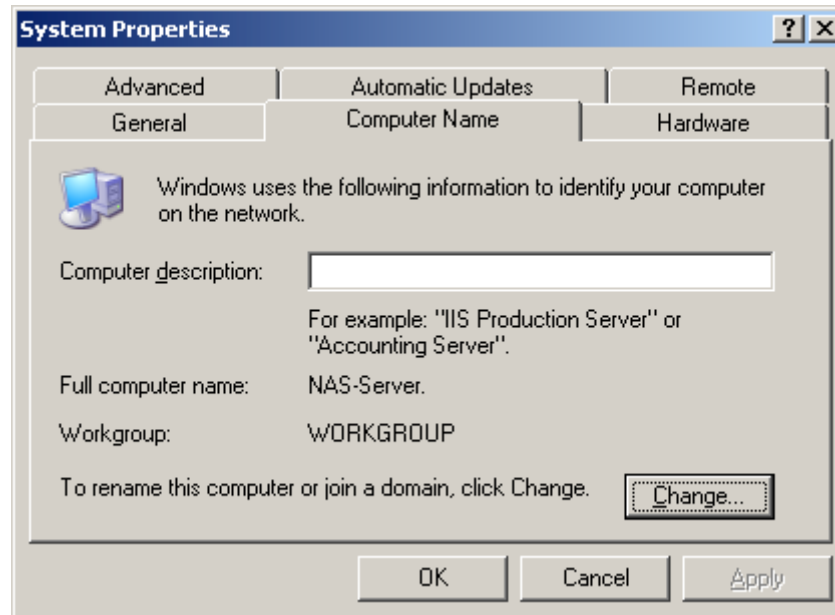
Fig. 134   "System Properties – Computer Name" dialog box

3.   Select the **Computer Name** tab.

4.   Click on **Change…**.

➔ The following dialog box opens.
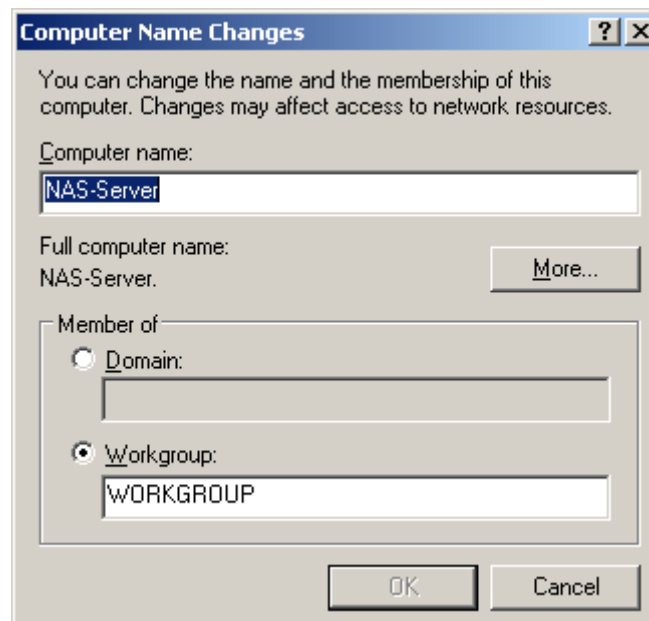
Fig. 135   "Computer Name Changes" dialog box

5.   Enter a name for the computer in the **Computer name** text field.

6.   To change the workgroup, enter the desired workgroup in the **Workgroup** text field.

7.   Click **OK**.

8.   Restart the computer.

Hard disk partitioning

ℹ️ Make sure that each partition on the NAS is larger than 250 GB.

1. Right-click on the desktop icon of the NAS Server.
2. Select **Manage**.
3. The **Computer Management** window will open.
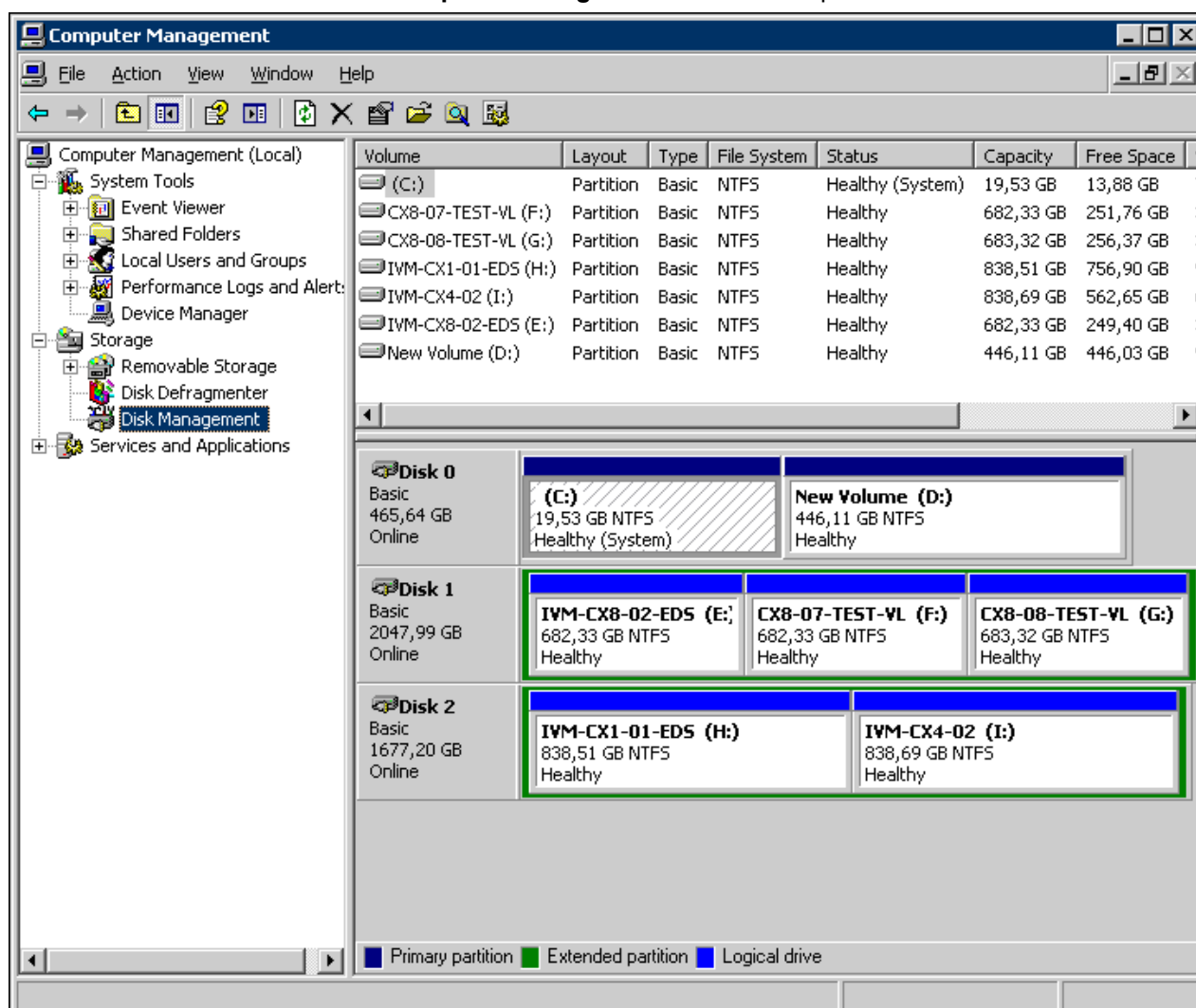
Fig. 136   Computer Management

4. Click **Disk Management** in the tree view.
5. Partition the hard disk.
6. Assign a drive letter and a name to each hard disk partition using NTFS.

Sharing a Network File System (NFS)

IMPORTANT	**Data loss due to crash of CX devices** If several SISTORE CX devices simultaneously access an NFS folder, this may result in a crash of the SISTORE CX devices. ● Create only one NFS folder per partition and CX device. ● We recommend using the name of the CX for the NFS folder and the IP address for the hard disk partition.

Please note that the name of the NFS folder is case-sensitive. The name will be used as the share name.

1. Create an NFS folder on the desired hard disk partition (e.g. CX1).

2. Right-click on the folder.

3. Select **Properties**.

➔ The following dialog box opens:

Fig. 137 "Properties – NFS Sharing" dialog box

4. Select the tab **NFS Sharing**.

5. Activate the option **Share this folder**.

➔ The share name corresponds with the name of the NFS folder and will be entered automatically.

The share name must be assigned only once.

6. Click on **Permissions**.

➔ The **NFS Share Permissions** dialog box opens.
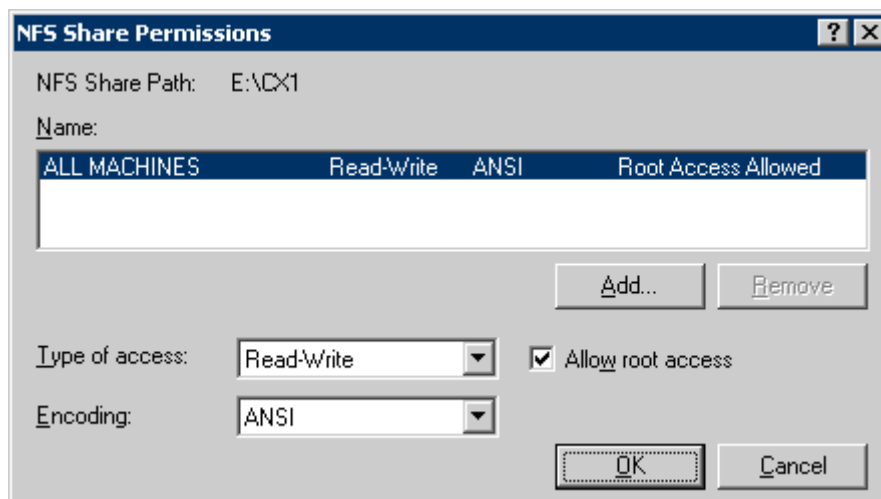
Fig. 138   "NFS Share Permissions" dialog box

7.   Click on **Add…**.

➔ The **Add Clients and Client Groups** dialog box opens.
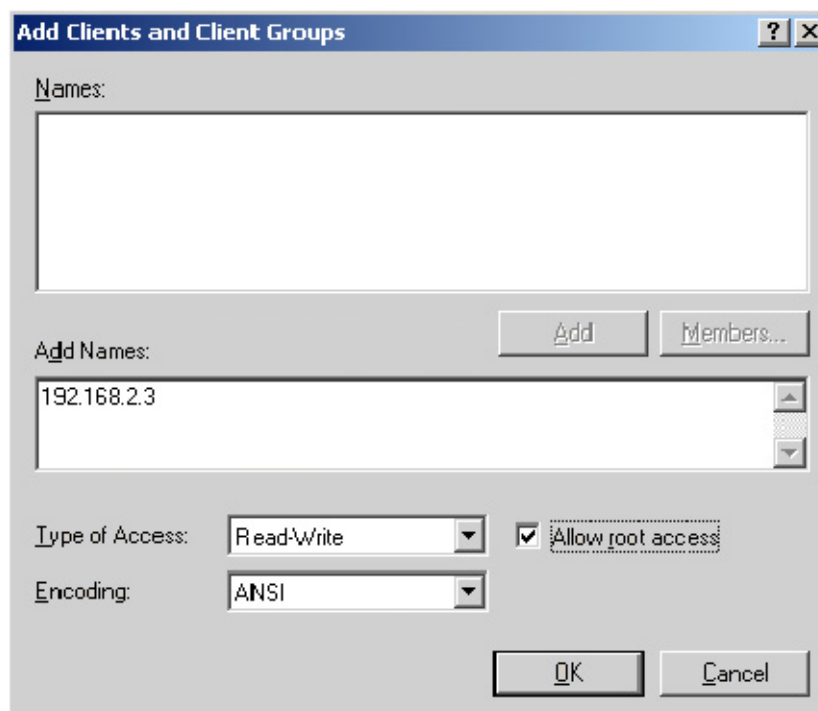
Fig. 139   "Add Clients and Client Groups" dialog box

8.   Enter the IP address of the CX device in the **Add Names** text field.

9.   Select **Read-Write** in the **Type of Access** list box.

10.   Mark the checkbox **Allow root access**.

11.   Click **OK**.

→ The IP address of the CX device will be displayed in the NFS Share Permissions dialog.
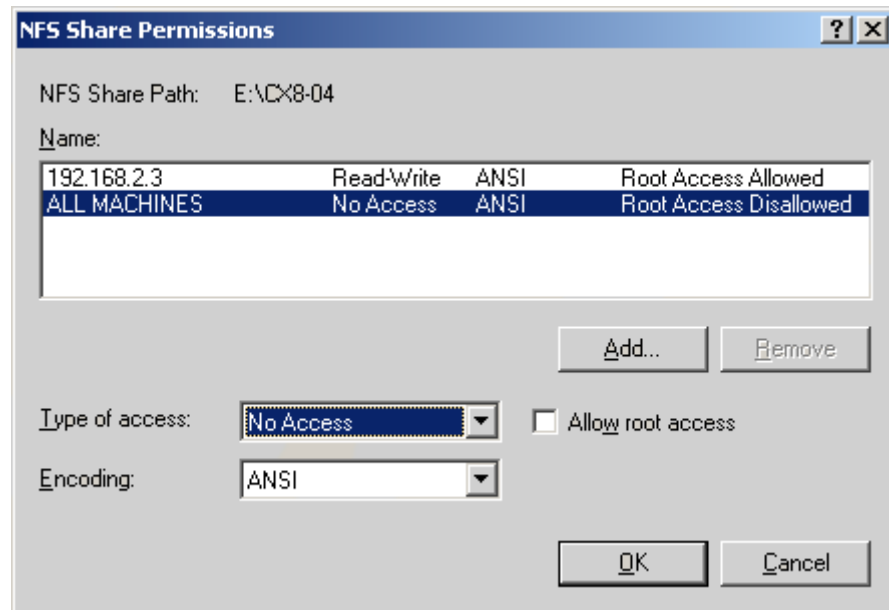
Fig. 140   "NFS Share Permissions" dialog box with IP address

12. Select **ALL MACHINES**.

13. Select **No Access** in the **Type of Access** list box.

14. Click **OK**.

→ The NFS can now be accessed only by the selected CX device.

15. To refresh the Explorer window, press **<F5>**.

→ The NFS appears in the Explorer window.

Assigning users and groups

i	The files **group** and **passwd** can be found on the client setup CD under CEVIS\Tools\nfs.

1. Save the files **group** and **passwd** locally on your computer.
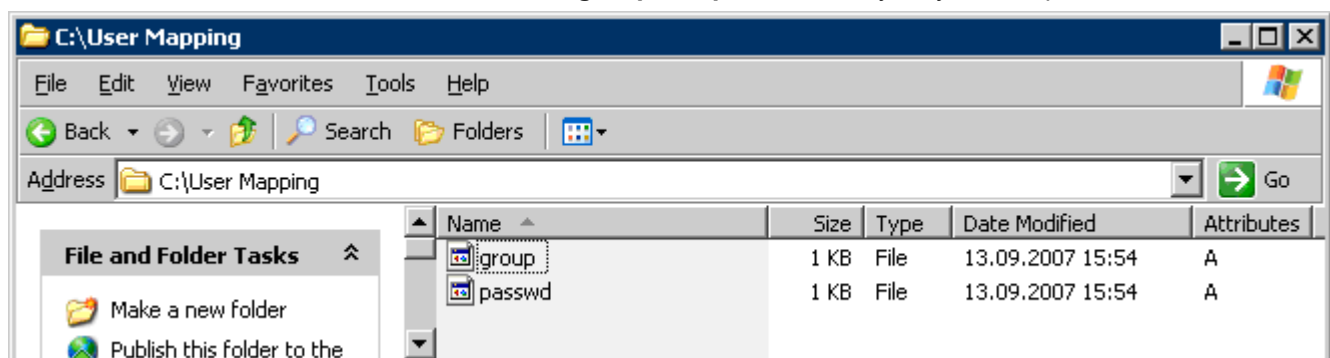
Fig. 141   Example of a local Windows directory

2. Select **Start** > **Settings > Control Panel** > **Administrative Tools** in the Windows start menu.

➔ The following window opens:
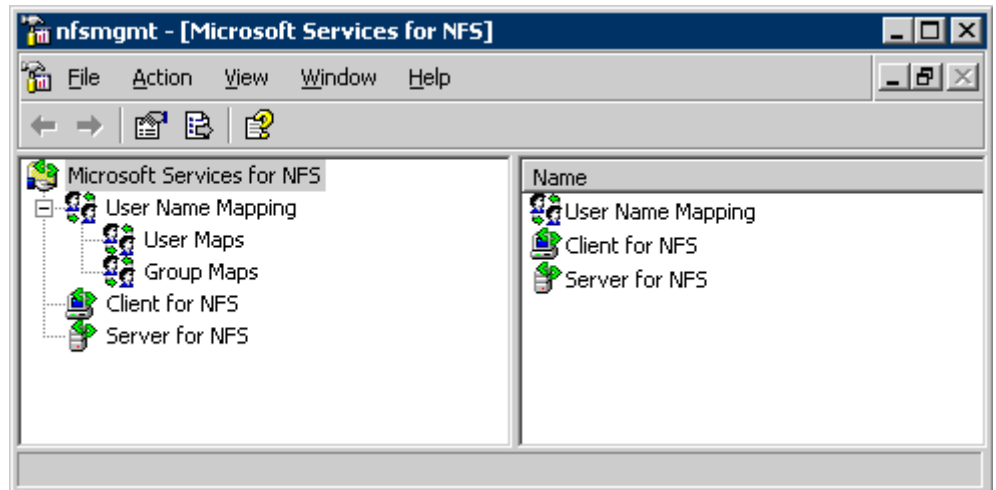
Fig. 142 Microsoft Services for NFS

Selecting a server name

1. Right-click on **Microsoft Services for NFS**.
2. Select **Properties**.
    ➔ The following dialog box opens:
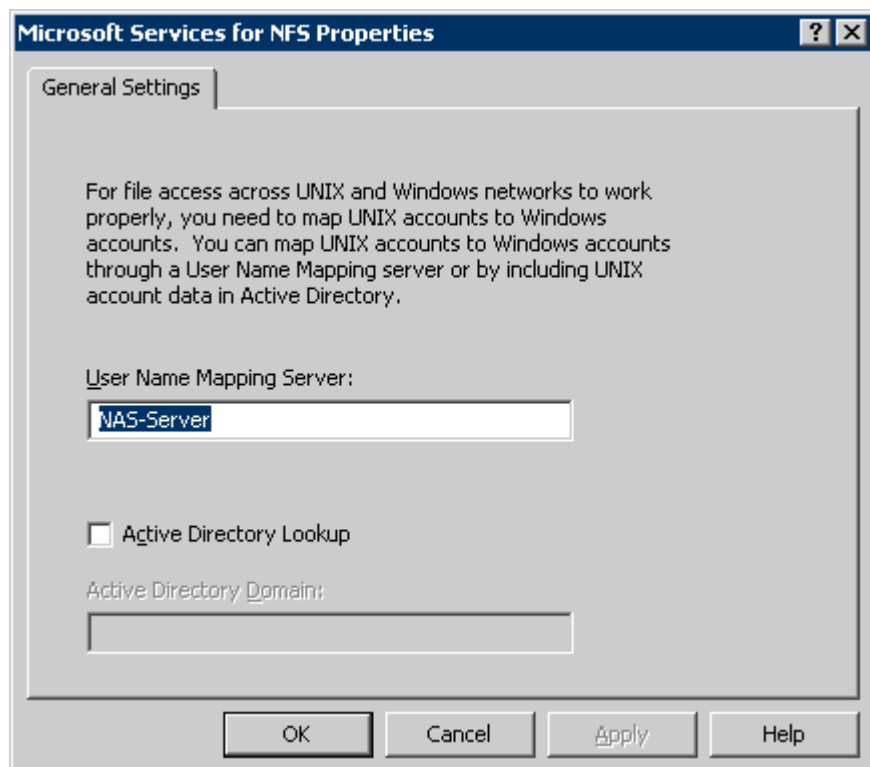
Fig. 143 "Microsoft Services for NFS Properties – General Settings" dialog box

3. Enter the server name in the **User Name Mapping Server** text field.
4. Click **OK**.

Using password and group files

1. Right-click on **User Name Mapping**.

2. Select **Properties**.

➔ The following dialog box opens:

3. Select the **UNIX User Source** tab.
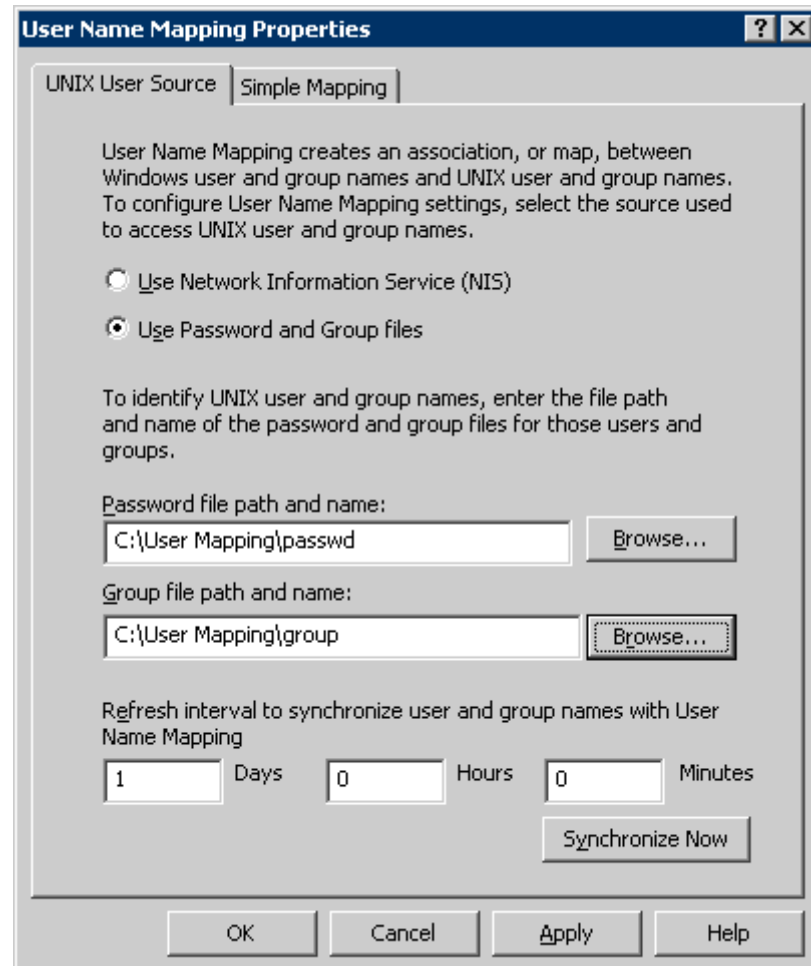
Fig. 144   "User Name Mapping Properties – UNIX User Source" dialog box

4. Activate the option **Use Password and Group files**.

5. In the field **Password file path and name**, select the path to the file **passwd** which you have stored locally on your computer.

6. In the field **Group file path and name**, select the path to the file **group** which you have stored locally on your computer.

7. Click on **Apply**.

8. Click **OK**.

Adding the user "root"

1. Right-click on **User Map**.

2. Select **Create Map**.

    ➔ The following dialog box opens:
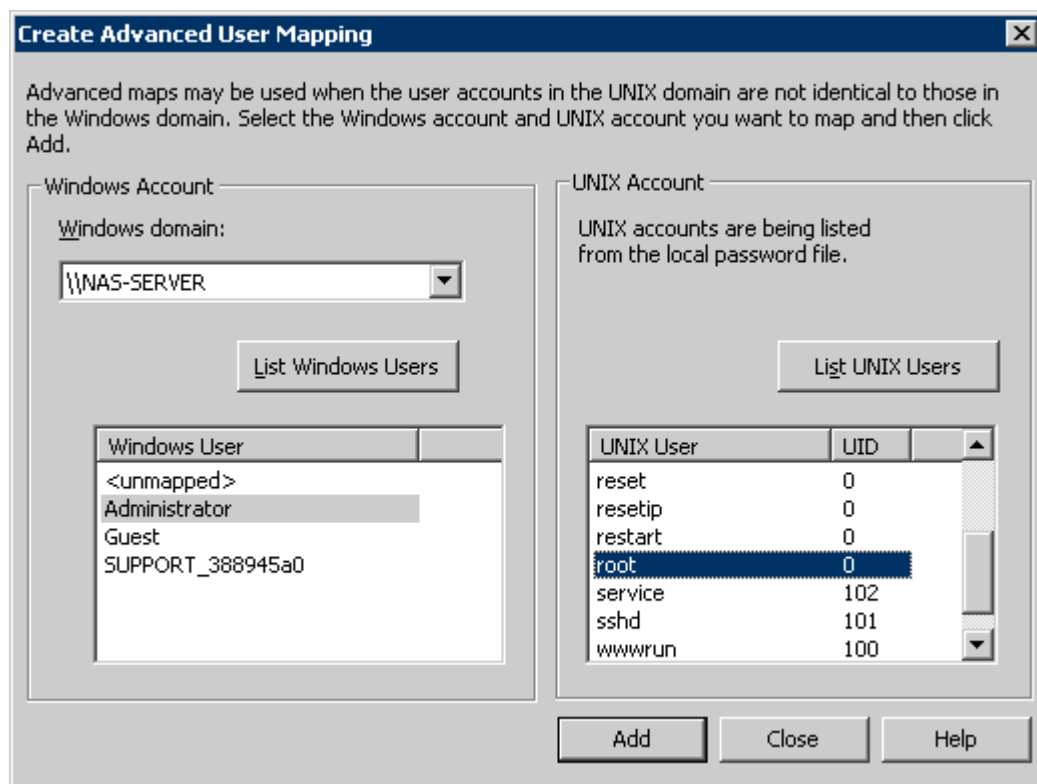
Fig. 145   "Create Advanced User Mapping" dialog box

3. Click on **List Windows Users**.

    ➔ All Windows users will be listed.

4. Select **Administrator**.

5. Click on **List UNIX Users**.

    ➔ All UNIX users will be listed.

6. Select **root**.
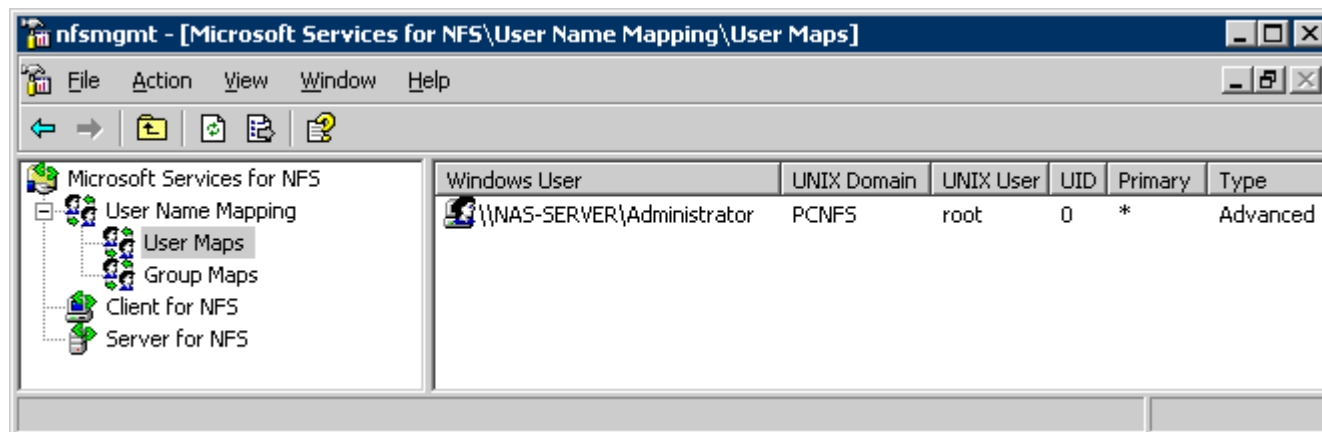
7. Click on **Add**.

Fig. 146   Added user

Adding the user "wwwrun"

1. Right-click on **User Map**.

2. Select **Create Map**.

   ➔ The **Create Advanced User Mapping** dialog box opens (see Fig. 145).

3. Select **Guest**.

4. Click on **List UNIX Users**.

   ➔ All UNIX users will be listed.

5. Select **wwwrun**.

6. Click on **Add**.

Assigning groups

1. Right-click on **Group Maps**.

2. Select **Create Map**.

   ➔ The following dialog box opens.
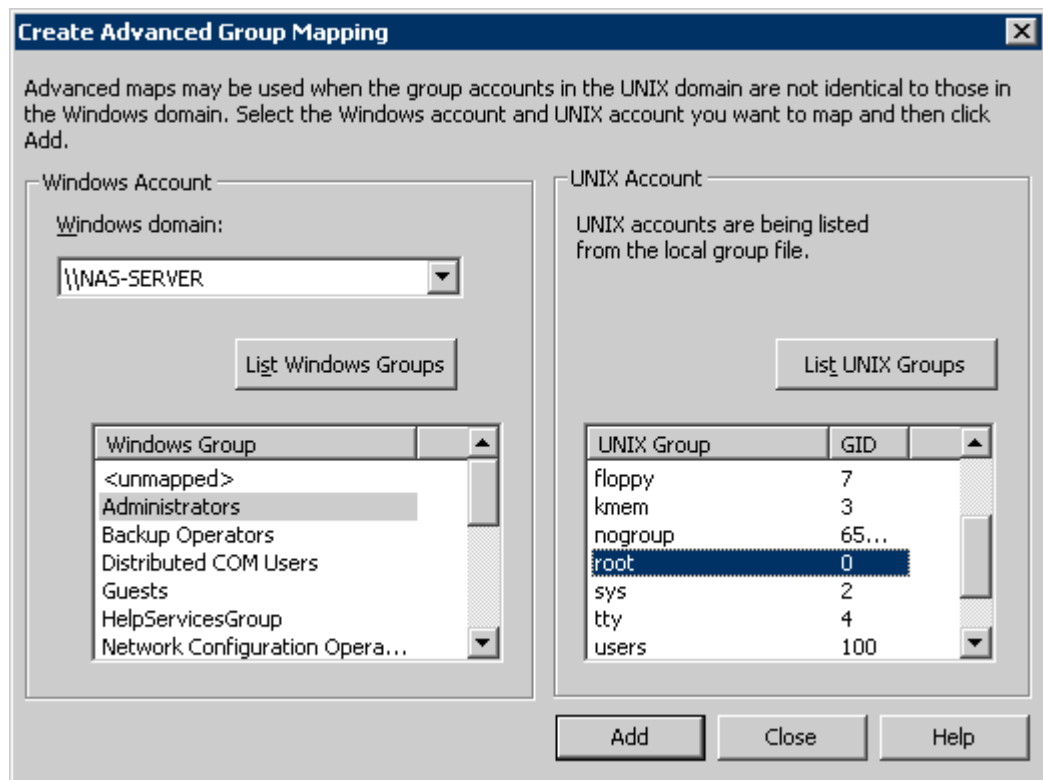
Fig. 147   "Create Advanced Group Mapping" dialog box

3. Click on **List Windows Groups**.

   ➔ All Windows groups will be listed.

4. Select **Administrator**.

5. Click on **List UNIX Groups**.

   ➔ All UNIX groups will be listed.

6. Select **root**.

7. Click on **Add**.
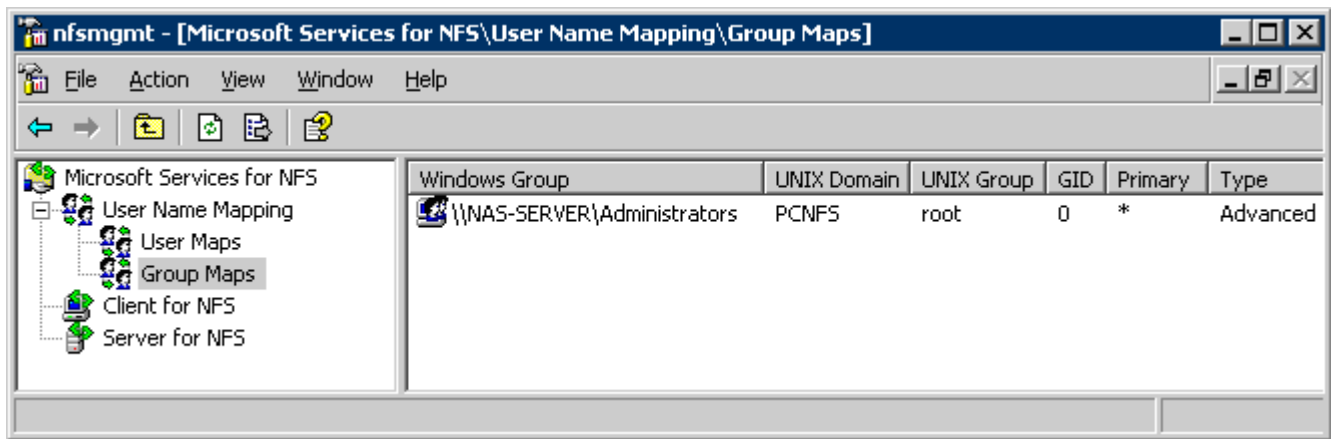
Fig. 148   Added group

Terminating configuration with Windows 2003 Storage Server

1. Close the window **Microsoft Services for NFS**.
2. Restart the server.

20.2   Configuring NAS using SISTORE CX Config

CX FDV

Prerequisite:

NAS has been configured with Windows 2003 Storage Server.

Activating NAS

Prerequisite:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

1. Start the SISTORE CX Config application. See Section: 3.15 Starting the software.
2. In the tree view, navigate to the node **Capacity**.
3. Select the **Capacity** tab.
4. Activate the option **Network Attached Storage**.
5. Click on **Apply**.
   → The SISTORE device will be restarted.

Assigning a device to a network connection

ℹ️ Since the NAS server has several network cards installed, we recommend assigning each device to a separate network connection.

Prerequisites:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

NAS has been activated.

1. Select the **NAS** tab.
   → The following dialog box opens.

Fig. 149   NAS – Assign network connection

2. Enter the IP address of the network connection in the **IP Address** text field.

ℹ️ Please note that the share name is case-sensitive. The share name corresponds with the name of the NFS folder (see Sharing a Network File System (NFS)).

3. Enter the share name in the **Share** text field.
4. Click **Apply**.
5. Answer **Yes** in the confirmation dialog.
   → The SISTORE device will be restarted.

21 Web interface

21.1 Opening the Web interface
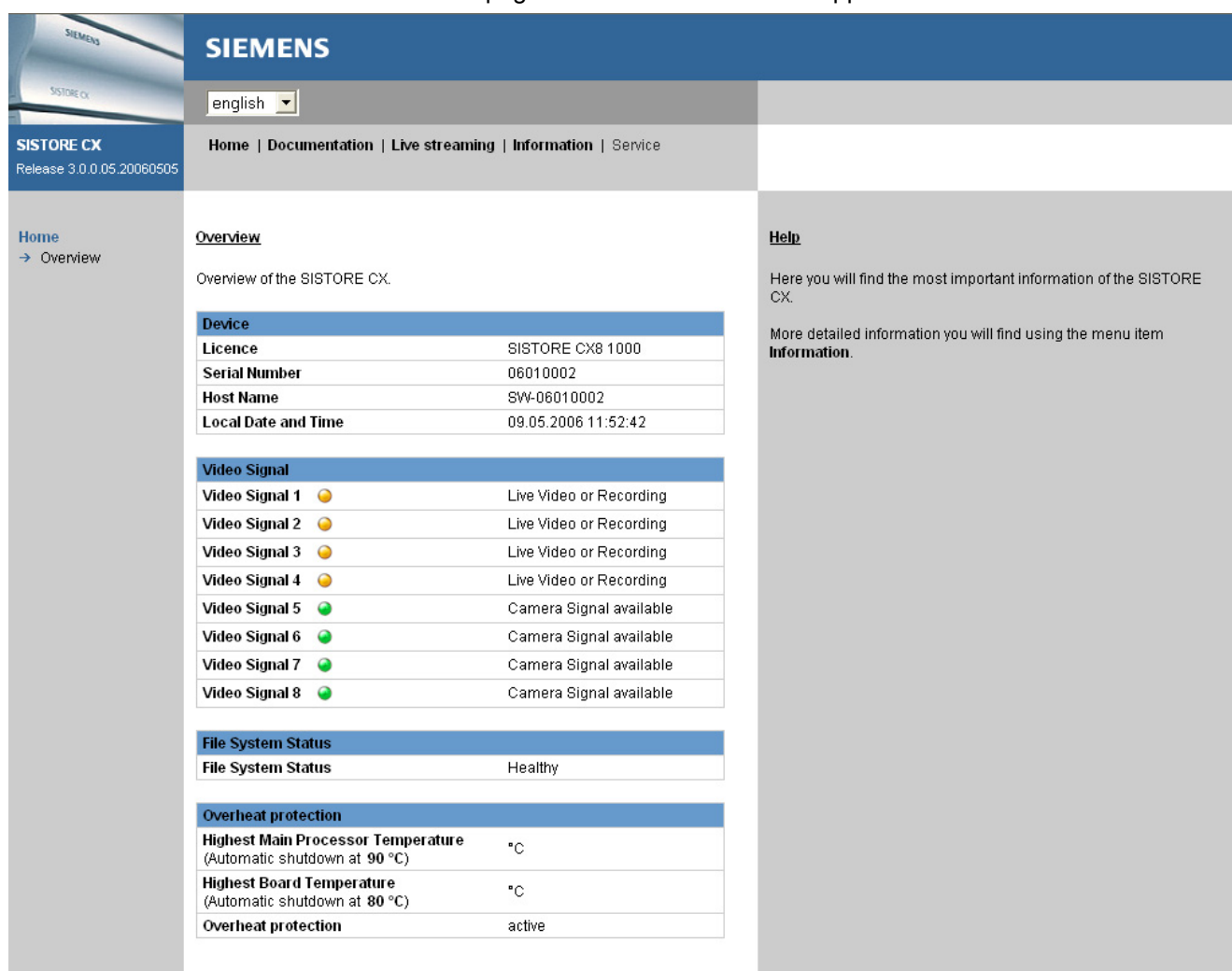
CX FDV

Prerequisites:

SISTORE CX Config has been started. See Section: 3.15 Starting the software.

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

1. In the tree view, navigate to a SISTORE device.
2. Click on the link next to **Home page**.
   ➔ The start page of the Web interface will appear.

Fig. 150 Web interface of the device

21.2 Displaying status information

CX FDV

You can access status information via the Web interface and via the configuration software SISTORE CX Config (see Section: 11 Configuring the storage medium).

Prerequisites:

A connection to the SISTORE device has been established. See Section: 4.1 Connecting to SISTORE device.

The Web interface of the SISTORE device has been opened. See Section: 21.1 Opening the Web interface.

1. Select **Information** in the main menu.
2. Select **HardDisk** in the submenu on the left.
    ➔ Depending on the hard disks available, the following status information will be displayed:

Compact Flash	
Model	Precise model designation
Revision	Version
Serial Number	Serial number
Capacity	Storage capacity

HardDisk	
Model	Precise model designation
Revision	Version
Serial Number	Serial number
Capacity	Storage capacity
S.M.A.R.T. status	Result of the hard disk check (see Section: 11.5 S.M.A.R.T. status).
Device	Designation of the device
Position	Position in the SISTORE device
Status	Hard disk status

Mirroring (RAID-1)	
R.A.I.D. status	Result of the hard disk mirror (see Section: 11.4 Mirroring internal hard disks).

Disk Array	
Device	Designation of the device
Status	Online or offline
Synchronization	The progress of the disk formatting process is shown here (see Section: 11.6 Changing the hard disk).

External SCSI Drive	
Status	Status indication - SCSI enabled or disabled
SCSI Adapter	Active RAID system, adapter detected
SCSI Device	Designation/type of device

21.3 Temperature management

CX FDV

Prerequisites:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

The Web interface of the SISTORE device has been opened. See Section:
21.1 Opening the Web interface.

1. Read all the information in the **Overheat protection** table on the start page.
2. Select **Information** in the main menu.
3. Select **Temperature** in the submenu.
4. Further statistics information can be found under **Temperature**.
5. Under **Overheat protection** you can see when the last emergency cutoff took place. See Section: 21.4 Last emergency cutout.

21.4 Last emergency cutout

CX FDV

Prerequisites:

A connection to the SISTORE device has been established. See
Section: 4.1 Connecting to SISTORE device.

The Web interface of the SISTORE device has been opened. See
Section: 21.1 Opening the Web interface.

1. Select **Information** in the main menu.
2. Select **Temperature** in the submenu.
3. Under **Overheat protection** you can see when the last emergency cutoff took place.

21.5 Displaying live video

CX FDV

Prerequisites:

You are using Internet Explorer 6.

Version 1.5.0_06 or higher of the Java Runtime Environments (JRE) is installed on the client PC.

In version 1.5.0_06 of the Java Runtime Environment the Java cache is deactivated.

Deactivating the Java cache

1. Select **Start** > **Settings** > **Control Panel** in the Windows start menu.
   → The **Control Panel** window will open.
2. Double click on **Java**.
   → The **Java Control Panel** dialog box will open.
3. Select the **General** tab.
4. Click on **View** in the **Temporary Internet Files** section.
5. Delete all existing entries.
6. Click **OK**.
7. Click on **Settings** in the **Temporary Internet Files** section.
8. Untick the checkbox **Activate caching**.
9. Close all open windows by clicking **OK**.
   → The Java cache is now deactivated.

Displaying live video

1. Select **Live video** in the main menu.
2. Select the desired video input in the submenu.
   → The following login dialog will appear.

Fig. 151   Web interface – Live video

3. Enter the user name and password for the device in the appropriate fields.
4. Click on **Login**.
   → The live video will be displayed.

22 The Scheduler

CX FDV

The scheduler allows time-controlled events to be executed. Events may be executed once or at regularly scheduled intervals. The scheduler also offers the possibility to define exceptions, when the event defined are not executed.

The scheduler is started by clicking on the button in the main window of SISTORE CX. When the scheduler is opened all details displayed are updated. The following module opens in the working area:
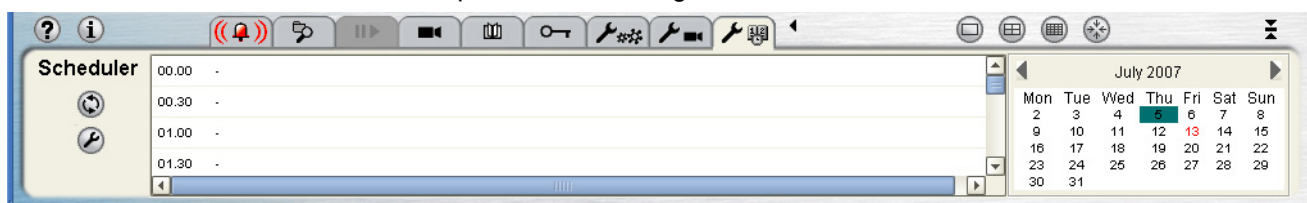
Fig. 152   Scheduler – Main screen

The scheduler dialog box is split into:

- Run
- Details on the selected day
- Calendar section for selecting the day

Run

This section allows various timing actions to be performed.

	Updating the schedule
	Entering a new schedule

Details on the selected day

In this section the actions which have been entered for the selected day are displayed. The vertical slider on the right can be used to navigate the selected day. The day is split into time windows of half an hour.

The information on scheduling is displayed as shown below:

Fig. 153   Scheduler - Display of schedules

ℹ   Multiple scheduled events in the same time window are separated by semi-colons. Recurring events are labelled with an *.

Calendar section for selecting the day

Fig. 154   Scheduler - Calendar

In this section there is a calendar with several functions:

- Navigation of the calendar
- Day selection for definition of scheduled events.
  The current day is displayed in red.
- Details of days on which scheduled events have been defined:
  - Dark green signifies a non-recurring event.
  - Bright green signifies a recurring event.

22.1   Adding a scheduled routine

CX FDV

Adding scheduled actions

An action is taken as being the scheduled execution of a SISTORE SX or CX rule. Scheduled actions are added using an assistant.

To do this, proceed as follows:

1.   Select the day on which the non-recurring action is to occur, or a recurring action is to begin, in the calendar.

Fig. 155   Scheduler - Day selection

2.   Now click on the icon **Add** .

➜ The following dialog box opens:
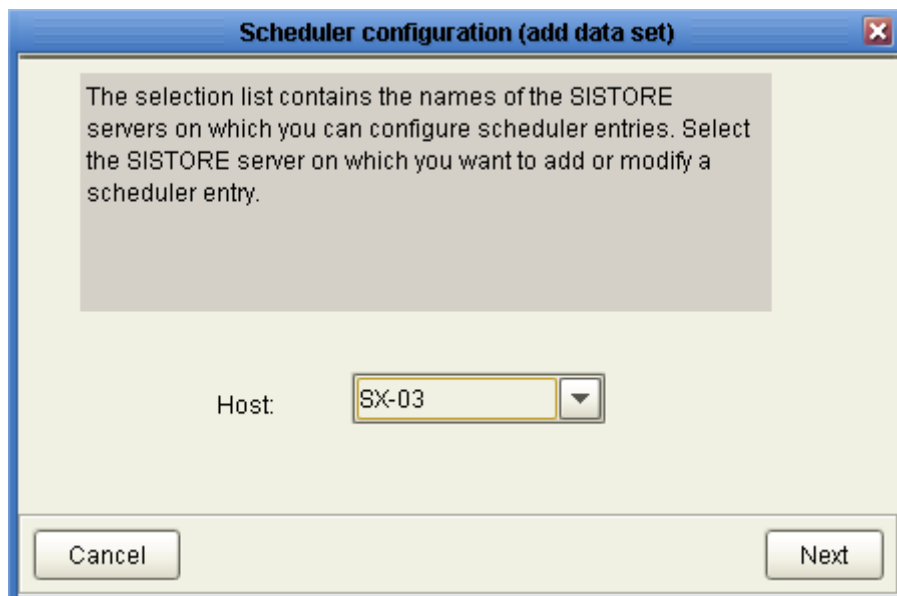
Fig. 156   Scheduler assistant - Server selection

3.   Select the SISTORE CX server on which the action should be executed in this dialog box.

> Multiple SISTORE CX servers are only displayed if they are added to the SISTORE device list. See Section: 4.1 Connecting to SISTORE device.

4.   Click **Next**.

→ The following dialog box opens:
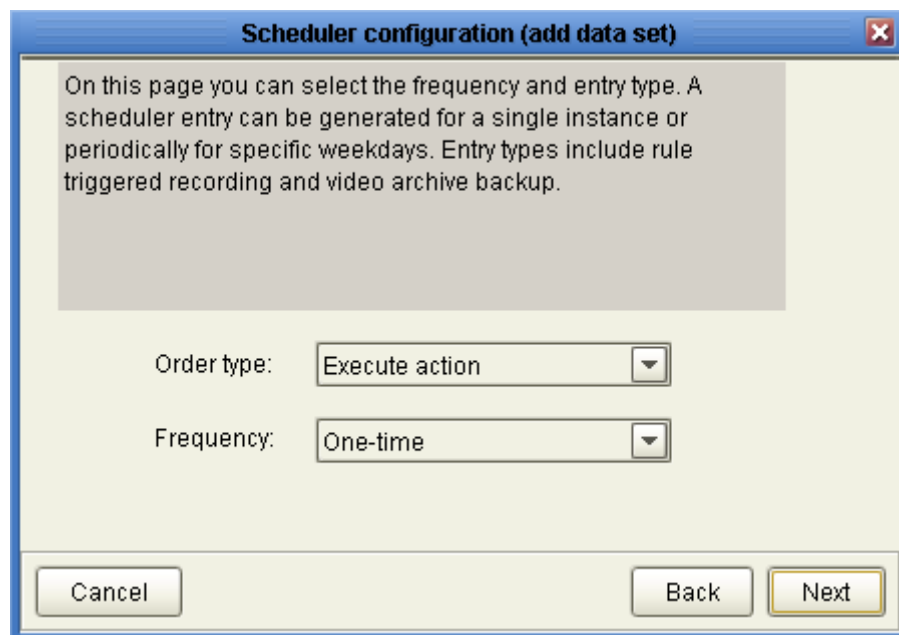
Fig. 157   Scheduler assistant - Selection of action / frequency

5.   In the **Order type** drop-down list select "Execute action".

6.   In the **Frequency** drop-down list you can choose either of the following two
actions:

– **One-time**, i.e. once at a specified time.

– **On appointed weekdays**, i.e. every week on a specified day at a specified
time.
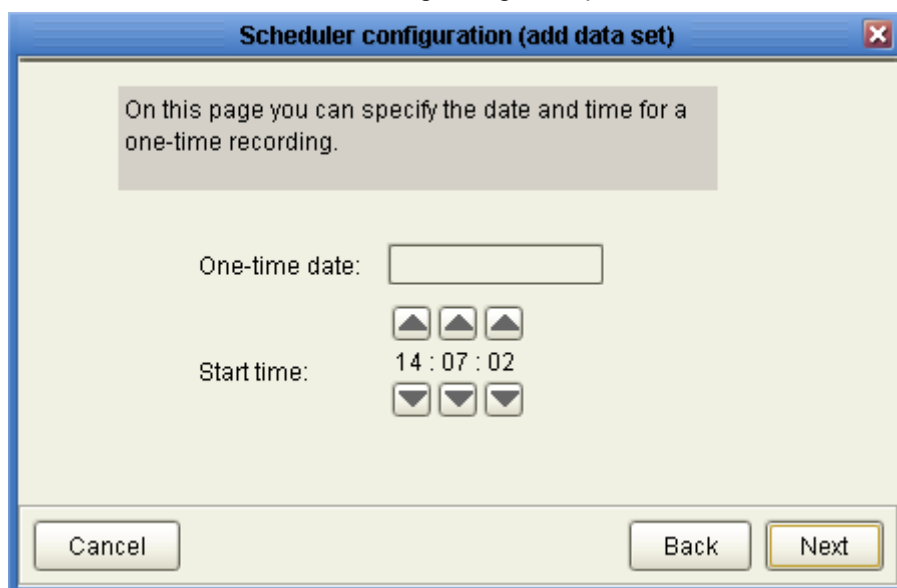
Depending on the selected frequency, different dialog boxes are opened by the assistant.

7.   Click **Next**.

Non-recurring event

➔ For this selection, the following dialog box opens:

Fig. 158   Scheduler assistant - Non-recurring event

1.   Click on the **One-time date** input field.

➔ This opens another calendar box, in which the day on which the event should be executed can be selected.
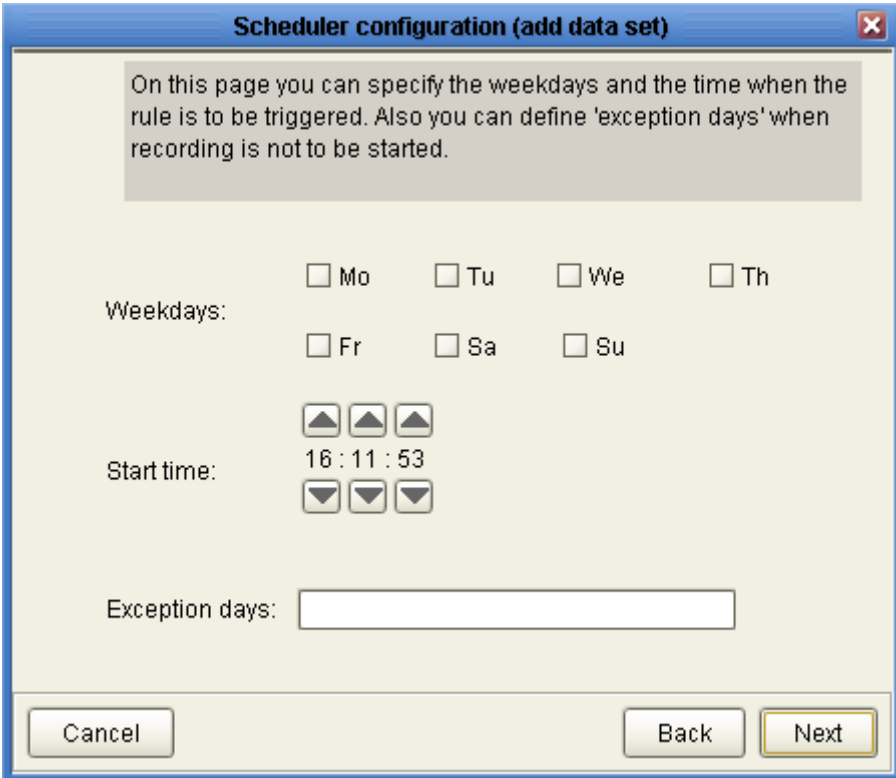
Fig. 159   Scheduler assistant - Non-recurring event / date

2.   Now select the date and define it with the navigation buttons below the date selection of the start time.

3.   Click **Next**.

On specific weekdays

➔ For this selection, the following dialog box opens:

Fig. 160   Scheduler assistant - Recurring event

1. To define the day(s) on which the event should be executed, mark the checkboxes of the appropriate week days.
2. Select the start time.
3. To specify exception days for an event, click on the **Exception days** input field.

   ➔ The calendar appears.

Fig. 161   Scheduler assistant - Recurring event / Exception days

4. Separate multiple exception days by semicolons.
5. Click **Next**.

➜ After selection and definition of the event type (non-recurring/recurring), the following dialog box will appear:
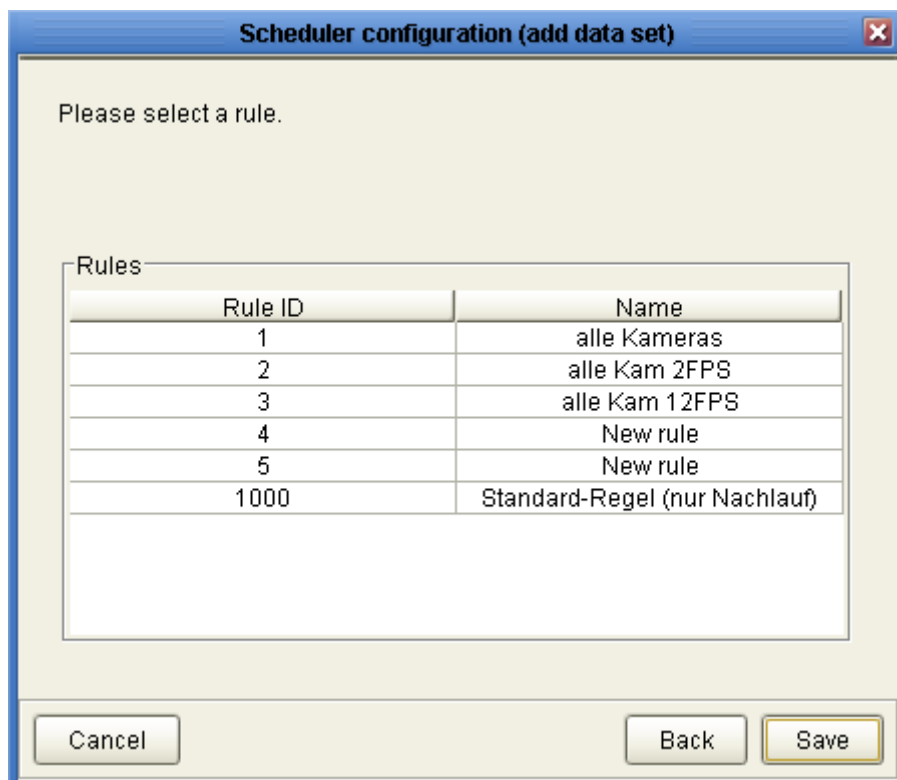
Fig. 162   Scheduler assistant – Rule selection

6. Select the rule which is to be launched by the event.

7. Click **Save**.

22.2   Editing a scheduled routine

CX FDV

Scheduled routines are edited by opening the scheduler and selecting the event to be changed in the calendar and the navigation within the day view.
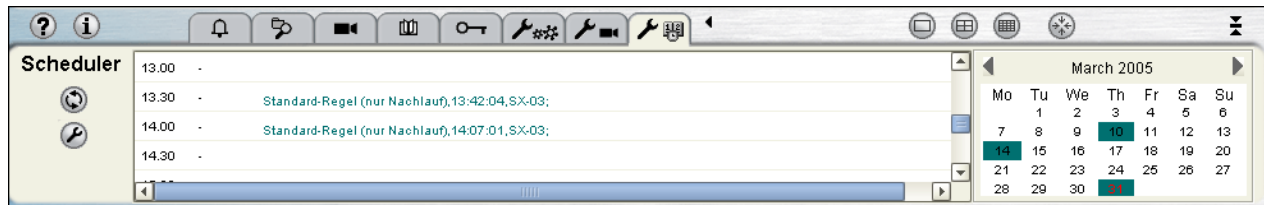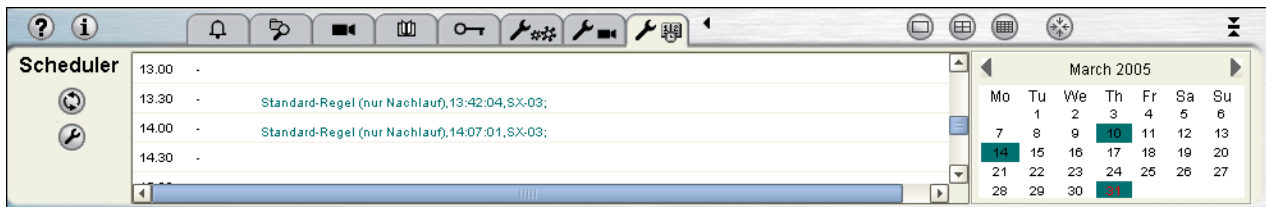

Fig. 163   Scheduler

1.   Position the mouse pointer over the entry and right-click.

2.   Choose **edit** from the pop-up menu.
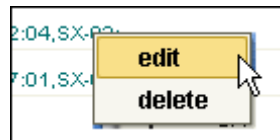
→ The following dialog box opens:
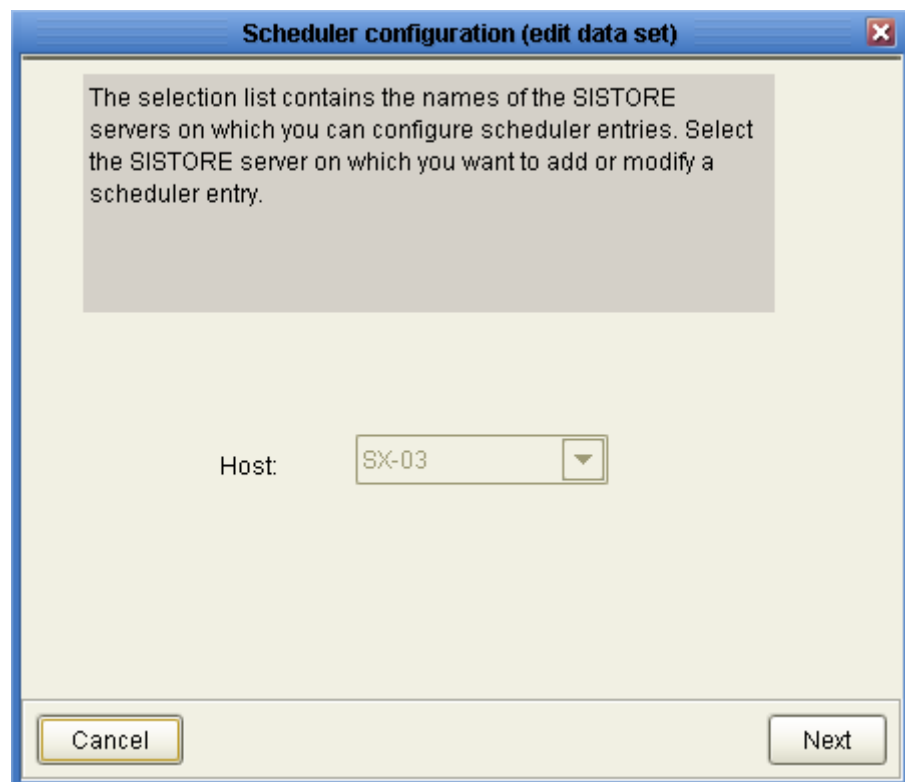
Fig. 164   Scheduler assistant

3.   The settings can now be changed as described in the previous chapter.

22.3   Deleting a scheduled routine

CX FDV

Scheduled routines are deleted by opening the scheduler and selecting the event to be deleted in the calendar and the navigation within the day view.

Fig. 165   Scheduler

1.   Click on the entry.

2.   Choose **delete** from the pop-up menu.
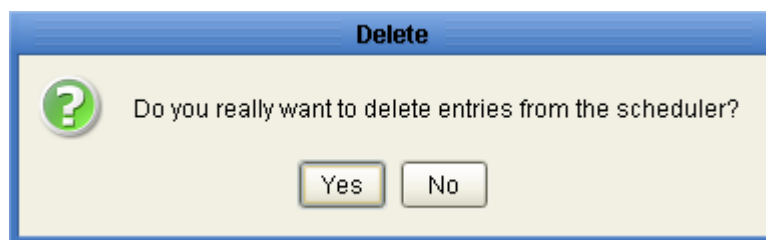

➔ The **Delete** dialog opens.

Fig. 166   Scheduler – Deletion confirmation alert

3.   Answer "Yes" in the confirmation box.

23 Disposal

All electrical and electronic products should be disposed of separately from the municipal waste stream via designated collection facilities appointed by the government or the local authorities.

This crossed-out wheeled bin symbol on the product means the product is covered by the European Directive 2002/96/EC.

The correct disposal and separate collection of your old appliance will help prevent potential negative consequences for the environment and human health. It is a precondition for reuse and recycling of used electrical and electronic equipment. For more detailed information about disposal of your old appliance, please contact your city office, waste disposal service or the shop where you purchased the product.

24   Appendix

24.1   User-defined start of the software

The software can be started using user-defined parameters in the software settings. A detailed description of the parameters can be found in the instruction manual for the VSS-SDK.

1.   Right-click on a desktop icon of the SISTORE CX software.

2.   Select **Properties** in the context menu.

3.   Select the **Shortcut** tab.

4.   If you wish to configure additional settings for the software start-up, add the appropriate parameters (see examples) in the **Target** command line.

5.   Click **Apply**.

Examples

● -<Action1><Value1> -<Action2><Value2>

The dash character "–" precedes each action, followed by a character for the **Action** and a string for the **Value** associated with this action. After that, there is a single space as a separator character for the next parameter. Spaces are allowed in the value. A space is only evaluated as a separator if it is followed by the dash character. No dashes are allowed in the value string.

Example:

–s141.76.23.3 –uAdministrator –m4

The parameters passed are the server name as an IP address, the user name and the command for start-up in 4-monitor view.

The following parameters can be passed when starting the application (the value is indicated by capital italic letters):

● –s*SERVERNAME*

Example: –s141.76.23.3

The server to which the client is to connect on starting can be specified as the name of the server or its IP address. The default value is "localhost".

● –u*USERNAME*

Example: –uAdmin

The user name for authentication on the server. An automatic login will be performed if the password and the server name or the IP address of the server are given as well.

● –p*PASSWORD*

Example: –pMyPassword

The password for user authentication on the server. An automatic login will be performed if the associated user name and the server name or the IP address of the server are given as well.

● –x*NoDirectShow*

Suppression of DirectX use.

● – i*LANGUAGE*

Example

–iEN   or: –iDE

International language code for the start-up language to be used regardless of the operating system.

With the exception of the *USERNAME* and *PASSWORD* parameters, all parameters can be used independently of one another. If the parameters *SERVERNAME*, *USERNAME* and *PASSWORD* are set, an automatic login will be performed. The user will not be asked for the user name, password, server name and port. If one of the parameters for login is not set, the login dialog will appear. Then the information must be completed.

i	A parameter that has not been set has either no value or its default value.

If the SISTORE CX Client is to be started as an applet (see the IVM WEB Client chapter), the following parameters must be used:

● PortID

The TCP/IP port on which the client should log in.

● UserName

The user name for authentication on the server.

● Password

The password for user authentication on the server.

Here is an example of parameter specification for the applet in HTML:

<PARAM NAME = PortID VALUE = "12050" >

<PARAM NAME = UserName VALUE = "admin" >

<PARAM NAME = Password VALUE = " admin " >

24.2   Supported image formats

The image files created by the SISTORE CX are based on MPEG-4 video technology. Four levels of resolution can be selected for the images stored in these files:

- **QCIF (176 x 144)**
  Quarter Common Intermediate Format
  Image format with a resolution 176 horizontal pixels and
  144 vertical pixels.

- **CIF (352 x 288)**
  Common Intermediate Format
  Image format with a resolution 352 horizontal pixels and
  288 vertical pixels.
  Originally developed for videophone and video conferencing services.

- **2CIF (704x288)**
  Double Common Intermediate Format
  Image format with a resolution 704 horizontal pixels and
  288 vertical pixels.
  The vertical pixels are doubled when displayed.

Deinterlacing formats

- **4CIF (704 x 576)**

  Quad Common Intermediate Format
  Image format with a resolution 704 horizontal pixels and
  576 vertical pixels.

- **DCIF (352 x 576)**

  Double Common Intermediate Format
  Image format with a resolution 352 horizontal pixels and
  576 vertical pixels.

Siemens Building Technologies
Fire Safety & Security Products

24.3 Network port assignment

Normal operation mode (SISTORE CX Client)

Port	Protocol	Description
12050	TCP	SISTORE CX Server <-> SISTORE CX Client
12051	TCP	SISTORE CX Server <-> SISTORE CX Client
12054	TCP	Firmware update SISTORE CX Server <-> SISTORE CX Config
23478	TCP	SISTORE CX Server <-> SISTORE CX Client (telemetry)
> 1024	TCP	Live video, dynamic port assignment SISTORE CX Server<-> SISTORE CX Client
8000-8031	RTP	Video stream – video protocol RTP Multicast SISTORE CX Server <-> SISTORE CX Client
12053	TCP	Alarm settings SISTORE CX Config <-> SISTORE CX Client

Configuration (SISTORE CX Config, SiADS Config)

Port	Protocol	Description
1900	UDP	"UPnP" functionality SISTORE CX <-> SISTORE CX Config (IP-Multicast address 239.255.255.250)
12054	TCP	Firmware update SISTORE CX Server <-> SISTORE CX Config
12055	TCP	Firmware update SISTORE CX Server <-> SISTORE CX Config
61975	TCP	Firmware update SISTORE CX Server <-> SISTORE CX Config
12060	TCP	DomainServer (optional) <-> SISTORE CX Config DomainServer (optional) <-> SISTORE CX Server

Other functions

Port	Protocol	Description
80	TCP	Homepage SISTORE CX Server
161	UDP	Information on the device via snmp (simple network management protocol)

Network Attached Storage (NAS)

Port	Protocol	Description
111	TCP	SUN RPC port mapping
2049	TCP/UDP	Network File System (NFS)
	TCP/UDP	NAS communication, dynamic assignment SISTORE CX Server<-> NAS

24.4   SISTORE CX network utilization and recording times

The following table provides information on the system performance of SISTORE CX that can be expected in a 100 Mbit/s network. The performance data refer to one camera in each case. The recording time will be divided among all the cameras connected to the system.

i   The values may differ by up to 30 %, depending on the image content.

Type of device				CX4 250	CX4 500	CX4 1000	CX8 500	CX8 1000
Usable storage capacity for recording video				195.8 GB	390.2 GB	780.3 GB	390.2 GB	780.3 GB
Image format	Image rate (ips)	Bandwidth (in MBit/s)	Quality	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)
4CIF	25.00	4.79	HHQ	93	185	371	185	371
4CIF	12.50	2.40	HHQ	186	370	741	370	741
4CIF	8.33	1.60	HHQ	279	556	1112	556	1112
4CIF	6.25	1.20	HHQ	372	741	1483	741	1483
4CIF	5.00	0.96	HHQ	465	927	1854	927	1854
4CIF	4.17	0.80	HHQ	558	1112	2224	1112	2224
4CIF	3.13	0.60	HHQ	744	1483	2965	1483	2965
4CIF	2.08	0.40	HHQ	1116	2224	4448	2224	4448
4CIF	1.00	0.19	HHQ	2326	4633	9266	4633	9266
4CIF	25.00	4.07	HQ	110	218	437	218	437
4CIF	12.50	2.10	HQ	213	424	847	424	847
4CIF	8.33	1.36	HQ	329	655	1310	655	1310
4CIF	6.25	1.02	HQ	439	874	1747	874	1747
4CIF	5.00	0.84	HQ	530	1056	2113	1056	2113
4CIF	4.17	0.68	HQ	658	1310	2621	1310	2621
4CIF	3.13	0.51	HQ	877	1747	3494	1747	3494
4CIF	2.08	0.34	HQ	1316	2621	5241	2621	5241
4CIF	1.00	0.16	HQ	2741	5460	10920	5460	10920
4CIF	25.00	3.60	STD	124	247	494	247	494
4CIF	12.50	1.80	STD	247	492	985	492	985
4CIF	8.33	1.20	STD	372	742	1483	742	1483
4CIF	6.25	0.90	STD	496	989	1978	989	1978
4CIF	5.00	0.72	STD	620	1236	2472	1236	2472
4CIF	4.17	0.60	STD	745	1483	2966	1483	2966
4CIF	3.13	0.45	STD	993	1978	3955	1978	3955
4CIF	2.08	0.30	STD	1489	2966	5933	2966	5933
4CIF	1.00	0.14	STD	3102	6180	12360	6180	12360
4CIF	25.00	3.00	LQ	149	296	592	296	592
4CIF	12.50	1.51	LQ	296	589	1179	589	1179
4CIF	8.33	1.00	LQ	446	888	1775	888	1775
4CIF	6.25	0.75	LQ	594	1183	2367	1183	2367
4CIF	5.00	0.60	LQ	741	1476	2951	1476	2951
4CIF	4.17	0.50	LQ	891	1775	3550	1775	3550
4CIF	3.13	0.38	LQ	1188	2367	4733	2367	4733
4CIF	2.08	0.25	LQ	1782	3550	7100	3550	7100
4CIF	1.00	0.12	LQ	3712	7396	14791	7396	14791
4CIF	25.00	2.41	LLQ	185	368	737	368	737
4CIF	12.50	1,21	LLQ	369	735	1471	735	1471
4CIF	8.33	0.80	LLQ	555	1105	2210	1105	2210
4CIF	6.25	0.60	LLQ	740	1473	2947	1473	2947

Type of device				CX4 250	CX4 500	CX4 1000	CX8 500	CX8 1000
Usable storage capacity for recording video				195.8 GB	390.2 GB	780.3 GB	390.2 GB	780.3 GB
Image format	Image rate (ips)	Bandwidth (in MBit/s)	Quality	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)
4CIF	5.00	0.49	LLQ	917	1826	3652	1826	3652
4CIF	4.17	0.40	LLQ	1109	2210	4420	2210	4420
4CIF	3.13	0.30	LLQ	1479	2947	5893	2947	5894
4CIF	2.08	0.20	LLQ	2219	4420	8840	4420	8840
4CIF	1.00	0.10	LLQ	4622	9209	18417	9209	18417
2CIF / DCIF	25.00	2.87	HHQ	155	309	618	309	618
2CIF / DCIF	12.50	1.44	HHQ	310	617	1234	617	1234
2CIF / DCIF	8.33	0.96	HHQ	465	926	1853	927	1853
2CIF / DCIF	6.25	0.72	HHQ	620	1235	2471	1235	2471
2CIF / DCIF	5.00	0.58	HHQ	774	1543	3086	1543	3086
2CIF / DCIF	4.17	0.48	HHQ	930	1853	3706	1853	3706
2CIF / DCIF	3.13	0.36	HHQ	1240	2471	4941	2471	4941
2CIF / DCIF	2.08	0.24	HHQ	1860	3706	7412	3706	7412
2CIF / DCIF	1.00	0.12	HHQ	3875	7720	15441	7720	15441
2CIF / DCIF	25.00	2.64	HQ	169	337	673	337	673
2CIF / DCIF	12.50	1.32	HQ	338	673	1345	673	1345
2CIF / DCIF	8.33	0.88	HQ	507	1010	2020	1010	2020
2CIF / DCIF	6.25	0.66	HQ	676	1346	2693	1346	2693
2CIF / DCIF	5.00	0.53	HQ	846	1685	3369	1685	3369
2CIF / DCIF	4.17	0.44	HQ	1014	2019	4039	2020	4039
2CIF / DCIF	3.13	0.33	HQ	1352	2693	5385	2693	5385
2CIF / DCIF	2.08	0.22	HQ	2027	4039	8078	4039	8078
2CIF / DCIF	1.00	0.11	HQ	4224	8414	16829	8415	16829
2CIF / DCIF	25.00	2.40	STD	186	371	742	371	742
2CIF / DCIF	12.50	1.20	STD	372	742	1483	742	1483
2CIF / DCIF	8.33	0.80	STD	558	1112	2225	1112	2225
2CIF / DCIF	6.25	0.60	STD	744	1483	2966	1483	2966
2CIF / DCIF	5.00	0.48	STD	929	1851	3703	1851	3703
2CIF / DCIF	4.17	0.40	STD	1117	2225	4449	2225	4449
2CIF / DCIF	3.13	0.30	STD	1489	2966	5932	2966	5932
2CIF / DCIF	2.08	0.20	STD	2233	4449	8898	4449	8898
2CIF / DCIF	1.00	0.10	STD	4653	9269	18538	9269	18538
2CIF / DCIF	25.00	2.04	LQ	219	435	871	435	871
2CIF / DCIF	12.50	1.02	LQ	437	871	1743	871	1743
2CIF / DCIF	8.33	0.68	LQ	655	1306	2611	1306	2611
2CIF / DCIF	6.25	0.51	LQ	874	1741	3482	1741	3482
2CIF / DCIF	5.00	0.41	LQ	1092	2175	4350	2175	4350
2CIF / DCIF	4.17	0.34	LQ	1311	2611	5223	2612	5223
2CIF / DCIF	3.13	0.25	LQ	1748	3482	6964	3482	6964
2CIF / DCIF	2.08	0.17	LQ	2622	5223	10446	5223	10446
2CIF / DCIF	1.00	0.08	LQ	5462	10881	21762	10881	21762
2CIF / DCIF	25.00	1.68	LLQ	265	527	1055	527	1055
2CIF / DCIF	12.50	0.84	LLQ	530	1055	2111	1055	2111
2CIF / DCIF	8.33	0.56	LLQ	794	1582	3164	1582	3164
2CIF / DCIF	6.25	0.42	LLQ	1059	2109	4218	2109	4218
2CIF / DCIF	5.00	0.34	LLQ	1325	2639	5278	2639	5278
2CIF / DCIF	4.17	0.28	LLQ	1588	3164	6327	3164	6327
2CIF / DCIF	3.13	0.21	LLQ	2117	4218	8436	4218	8436
2CIF / DCIF	2.08	0.14	LLQ	3176	6327	12654	6327	12655
2CIF / DCIF	1.00	0.07	LLQ	6617	13182	26364	13182	26364
CIF	25.00	2.39	HHQ	187	372	744	372	744

248

Type of device				CX4 250	CX4 500	CX4 1000	CX8 500	CX8 1000
Usable storage capacity for recording video				195.8 GB	390.2 GB	780.3 GB	390.2 GB	780.3 GB
Image format	Image rate (ips)	Bandwidth (in MBit/s)	Quality	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)
CIF	12.50	1.19	HHQ	374	746	1491	746	1491
CIF	8.33	0.80	HHQ	560	1116	2232	1116	2232
CIF	6.25	0.60	HHQ	747	1488	2977	1488	2977
CIF	5.00	0,48	HHQ	937	1866	3732	1866	3732
CIF	4.17	0.40	HHQ	1121	2232	4465	2232	4465
CIF	3.13	0.30	HHQ	1494	2977	5953	2977	5953
CIF	2.08	0.20	HHQ	2241	4465	8930	4465	8930
CIF	1.00	0.10	HHQ	4669	9302	18603	9302	18603
CIF	25.00	1.79	HQ	249	497	993	497	993
CIF	12.50	0.90	HQ	499	995	1990	995	1990
CIF	8.33	0.60	HQ	748	1490	2979	1490	2979
CIF	6.25	0.45	HQ	997	1986	3972	1986	3972
CIF	5.00	0.36	HQ	1247	2484	4969	2484	4969
CIF	4.17	0.30	HQ	1495	2979	5958	2979	5958
CIF	3.13	0.22	HQ	1994	3972	7944	3972	7944
CIF	2.08	0.15	HQ	2991	5958	11916	5958	11916
CIF	1.00	0.072	HQ	6231	12413	24826	12413	24826
CIF	25.00	1,19	STD	374	745	1490	745	1490
CIF	12.50	0.60	STD	746	1486	2972	1486	2972
CIF	8.33	0.40	STD	1122	2234	4468	2234	4468
CIF	6.25	0.30	STD	1495	2979	5958	2979	5958
CIF	5.00	0.24	STD	1859	3704	7409	3704	7409
CIF	4.17	0.20	STD	2243	4468	8937	4468	8937
CIF	3.13	0.15	STD	2991	5958	11916	5958	11916
CIF	2.08	0.10	STD	4486	8937	17874	8937	17874
CIF	1.00	0.05	STD	9346	18618	37237	18618	37237
CIF	25.00	0.96	LQ	465	927	1854	927	1854
CIF	12.50	0.48	LQ	931	1855	3710	1855	3710
CIF	8.33	0.32	LQ	1396	2781	5562	2781	5562
CIF	6.25	0.24	LQ	1861	3708	7416	3708	7416
CIF	5.00	0.19	LQ	2323	4628	9255	4628	9255
CIF	4.17	0.16	LQ	2792	5562	11124	5562	11124
CIF	3.13	0.12	LQ	3723	7416	14832	7416	14832
CIF	2.08	0.08	LQ	5584	11124	22248	11124	22248
CIF	1.00	0.04	LQ	11633	23175	46351	23175	46351
CIF	25.00	0.72	LLQ	617	1229	2458	1229	2458
CIF	12.50	0.36	LLQ	1235	2460	4920	2460	4920
CIF	8.33	0.24	LLQ	1850	3686	7373	3686	7373
CIF	6.25	0.18	LLQ	2467	4915	9830	4915	9830
CIF	5.00	0.14	LLQ	3081	6138	12276	6138	12276
CIF	4.17	0.12	LLQ	3701	7373	14745	7373	14745
CIF	3.13	0.09	LLQ	4934	9830	19660	9830	19660
CIF	2.08	0.06	LLQ	7402	14745	29490	14745	29490
CIF	1.00	0.03	LLQ	15420	30719	61438	30719	61438
QCIF	25.00	1.20	HHQ	371	739	1478	739	1478
QCIF	12.50	0.60	HHQ	742	1479	2958	1479	2958
QCIF	8.33	0.40	HHQ	1113	2217	4434	2217	4434
QCIF	6.25	0.30	HHQ	1484	2956	5911	2956	5911
QCIF	5.00	0.24	HHQ	1857	3700	7400	3700	7400
QCIF	4.17	0.20	HHQ	2226	4434	8867	4434	8867
QCIF	3.13	0.15	HHQ	2967	5911	11823	5911	11823
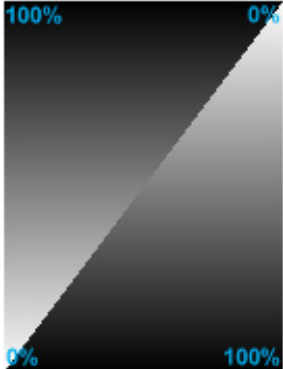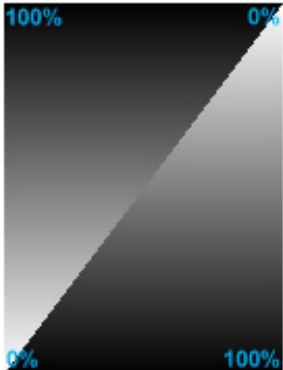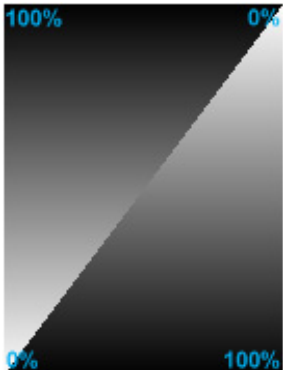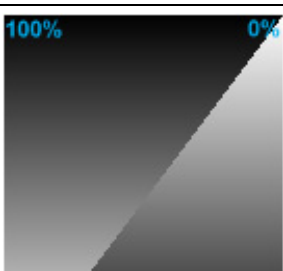
Siemens Building Technologies

Fire Safety & Security Products

Appendix

Type of device				CX4 250	CX4 500	CX4 1000	CX8 500	CX8 1000
Usable storage capacity for recording video				195.8 GB	390.2 GB	780.3 GB	390.2 GB	780.3 GB
Image format	Image rate (ips)	Bandwidth (in MBit/s)	Quality	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)	Rec. time (in h)
QCIF	2.08	0.10	HHQ	4451	8867	17734	8867	17734
QCIF	1.00	0.05	HHQ	9273	18473	36946	18473	36946
QCIF	25.00	0.96	HQ	465	927	1854	927	1854
QCIF	12.50	0,48	HQ	933	1858	3717	1858	3717
QCIF	8.33	0.32	HQ	1396	2781	5563	2781	5563
QCIF	6.25	0.24	HQ	1862	3709	7417	3709	7417
QCIF	5.00	0.19	HQ	2331	4645	9289	4645	9289
QCIF	4.17	0.16	HQ	2792	5563	11126	5563	11126
QCIF	3.13	0.12	HQ	3723	7417	14834	7417	14834
QCIF	2.08	0.08	HQ	5585	11126	22251	11126	22251
QCIF	1.00	0.04	HQ	11634	23178	46356	23178	46356
QCIF	25.00	0.72	STD	620	1236	2471	1236	2471
QCIF	12.50	0.36	STD	1242	2475	4949	2475	4949
QCIF	8.33	0.24	STD	1861	3707	7413	3707	7413
QCIF	6.25	0.18	STD	2481	4942	9885	4942	9885
QCIF	5.00	0.14	STD	3109	6193	12386	6193	12386
QCIF	4.17	0.12	STD	3721	7413	14827	7413	14827
QCIF	3.13	0.09	STD	4962	9885	19769	9885	19769
QCIF	2.08	0.06	STD	7443	14827	29654	14827	29654
QCIF	1.00	0.03	STD	15505	30889	61778	30889	61778
QCIF	25.00	0,48	LQ	933	1858	3716	1858	3716
QCIF	12.50	0.24	LQ	1864	3714	7427	3714	7427
QCIF	8.33	0.16	LQ	2798	5574	11148	5574	11148
QCIF	6.25	0.12	LQ	3731	7432	14864	7432	14864
QCIF	5.00	0.10	LQ	4663	9290	18580	9290	18580
QCIF	4.17	0.08	LQ	5596	11148	22296	11148	22296
QCIF	3.13	0.06	LQ	7461	14864	29728	14864	29728
QCIF	2.08	0.04	LQ	11192	22296	44592	22296	44592
QCIF	1.00	0.02	LQ	23316	46450	92899	46450	92899
QCIF	25.00	0.24	LLQ	1870	3725	7450	3725	7450
QCIF	12.50	0.12	LLQ	3726	7423	14845	7423	14845
QCIF	8.33	0.08	LLQ	5610	11176	22351	11176	22351
QCIF	6.25	0.06	LLQ	7480	14901	29802	14901	29802
QCIF	5.00	0.05	LLQ	9286	18499	36998	18499	36998
QCIF	4.17	0.04	LLQ	11219	22351	44702	22351	44702
QCIF	3.13	0.03	LLQ	14959	29802	59603	29802	59603
QCIF	2.08	0.02	LLQ	22439	44702	89404	44702	89404
QCIF	1.00	0.01	LLQ	46747	93130	186259	93130	186259

24.5 Frame rate with Dual Encoding

With dual encoding, the following maximum frame rates apply to streaming and recording (at 4CIF resolution).

The maximum frame rates for other resolutions can be obtained by multiplication with the following factors:

- 2CIF - frame rate in the table x 2.08
- DCIF - frame rate in the table x 1.50
- CIF - frame rate in the table x 4.16
- QCIF - frame rate in the table x 8.00

Operating mode	Streaming	Encoder reservation	Recording
Standard-performance encoder: SISTORE CX4: 4 video inputs SISTORE CX8: 8 video inputs	1 ips	100% … 0%	12.5 ips
	1 ips		8.33 ips
	2.08 ips		8.33 ips
	3.12 ips		8.33 ips
	5 ips		6.25 ips
	6.25 ips		6.25 ips
	6.25 ips		5 ips
	8.33 ips		3.12 ips
	8.33 ips		2.08 ips
	8.33 ips		1 ips
	12.5 ips	0% … 100%	1 ips
Enhanced-performance encoder: SISTORE CX4: 2 video inputs SISTORE CX8: 4 video inputs SISTORE CX1: 1 video input	1 ips	100% … 0%	25 ips
	2.08 ips		12.5 ips
	5 ips		12.5 ips
	6.25 ips		12.5 ips
	8.33 ips		12.5 ips
	12.5 ips		12.5 ips
	12.5 ips		8.33 ips
	12.5 ips		6.25 ips
	12.5 ips		5 ips
	12.5 ips		2.08 ips
	25 ips	0% … 100%	1 ips
EDS enhanced-performance tracking and encoder: SISTORE CX1: 1 video input SISTORE CX4: 2 video inputs SISTORE CX8: 4 video inputs	1 ips	100% … 0%	2.08 ips
	1 ips		1 ips
	2.08 ips	0% … 100%	1 ips
EDS standard-performance tracking and encoder: SISTORE CX1: 2 video inputs SISTORE CX4: 2 video inputs SISTORE CX8: 4 video inputs	1 ips	100% … 0%	5 ips
	1 ips		4.16 ips
	2.08 ips		3.12 ips
	3.12 ips		3.12 ips
	3.12 ips		2.08 ips

Operating mode	Streaming	Encoder reservation	Recording
	4.16 ips		1 ips
	5 ips		1 ips
EDS standard-performance tracking and encoder: SISTORE CX4: 4 video inputs SISTORE CX8: 8 video inputs	1 ips		1 ips
ODR and standard-performance encoder: SISTORE CX1: 1 video input	1 ips		5 ips
	1 ips		4.16 ips
	2.08 ips		3.12 ips
	3.12 ips		3.12 ips
	3.12 ips		2.08 ips
	4.16 ips		1 ips
	5 ips		1 ips
ODR and standard-performance encoder: SISTORE CX4: 4 video inputs SISTORE CX8: 8 video inputs	1 ips		1 ips

25 Glossary

Image sensor	Camera - CCD image sensor - CMOS image sensor - Tube camera
Blooming effects	"Bright patches" on the screen resulting from interference (electron overflow) between adjacent pixels on CCD image sensors.
Homography	A geometrical transformation of a two-dimensional image into a projection fitted perfectly into a defined setting.
Post-event recording	Designation for recorded video sequences taken after an event occurs.
Projection	See homography
ROI	Region Of Interest
Smearing effects	Vertical streaking on the image as a result of interference between adjacent pixels on CCD image sensors, caused by car headlights, for example (so-called highlights).
Teaming	Teaming provides redundancy of physical network connections between Switch and NAS by establishing a logical network connection between these.
Target bit rate	Measure of the image quality. The following bit rates are defined for SISTORE CX: **CIF** 30.000: Lowest image quality 40.000: Low image quality 50.000: Standard image quality 75.000: High image quality 100.000: Highest image quality **2CIF / DCIF** 70.000: Lowest image quality 85.000: Low image quality 100.000: Standard image quality 110.000: High image quality 120.000: Highest image quality
Tracking	Tracking is the pursuit of a moving object. In the context of event detection it is the pursuit of a vehicle, for example.
Pre-event recording	Designation for video sequences from the ring buffer that record the history prior to an event.

26 List of abbreviations

CCTV	Closed Circuit Television
DSP	Digital signal processor
FDnet	Field device network fire detection
FFFR	Full frame full rate
HHQ	Highest quality
HQ	High quality
ips	Images per second
IVM	Interactive Video Management
LQ	Low quality
LLQ	Lowest quality
NAS	Network-attached storage
NFS	Network File System
STD	Default image quality
VKS	Video matrix switcher

27   Index